BOIES SCHILLER FLEXNER LLP
David Boies (admitted pro hac vice)
333 Main Street
Armonk, NY 10504
Tel: (914) 749-8200
dboies@bsfllp.com

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
mmao@bsfllp.com
brichardson@bsfllp.com

James Lee (admitted pro hac vice)
Rossana Baeza (admitted pro hac vice)
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
jlee@bsfllp.com
rbaeza@bsfllp.com

Alison L. Anderson, CA Bar No. 275334
M. Logan Wright
725 S Figueroa St., 31st Floor
Los Angeles, CA 90017
Tel.: (213) 995-5720
alanderson@bsfllp.com
mwright@bsfllp.com

SUSMAN GODFREY L.L.P.
Bill Carmody (admitted pro hac vice)
Shawn J. Rabin (admitted pro hac vice)
Steven M. Shepard (admitted pro hac vice)
Alexander Frawley (admitted pro hac vice)
Ryan Sila (admitted pro hac vice)
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel.: (212) 336-8330
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com
afrawley@susmangodfrey.com
rsila@susmangodfrey.com

Amanda K. Bonn, CA Bar No. 270891
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel.: (310) 789-3100
abonn@susmangodfrey.com

MORGAN & MORGAN
John A. Yanchunis (admitted pro hac vice)
Ryan J. McGee (admitted pro hac vice)
Michael F. Ram, CA Bar No. 104805
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com
mram@forthepeople.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, SAL CATALDO, JULIAN SANTIAGO, and SUSAN LYNN HARVEY individually and on behalf of all other similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No.: 3:20-cv-04688-RS

DECLARATION OF JONATHAN HOCHMAN IN SUPPORT OF PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

Judge: Hon. Richard Seeborg
Courtroom 3 – 17th Floor
Date: October 5, 2023
Time: 1:30 p.m.

DECLARATION OF JONATHAN HOCHMAN

I, Jonathan Hochman, declare as follows.

1. Counsel for the *Rodriguez* Plaintiffs retained me to provide expert analysis and, if requested, expert testimony. I have personal knowledge of the matters set forth herein and am competent to testify.

2. I submit this declaration in connection with Plaintiffs' Motion for Class Certification.

3. Attached is a true and correct copy of the Expert Report that I prepared in connection with this matter, dated March 22, 2023. The opinions I provided therein are true and correct to the best of my knowledge.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 17th day of July, 2023, at New London, CT

/s/ Jonathan E. Hochman

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, SAL CATALDO, JULIAN SANTIAGO, and SUSAN LYNN HARVEY, individually and on behalf of all other similarly situated,	§	
Plaintiffs,	§	**Case No. 3:20-cv-04688-RS**
v.	§	
GOOGLE LLC,	§	
Defendant.	§	

EXPERT REPORT OF JONATHAN E. HOCHMAN

March 22, 2023

Portions Designated Highly Confidential – Attorneys' Eyes Only by Plaintiffs (blue highlights)

Table of Contents

I. INTRODUCTION

1. When the first iPhone launched in 2007—just 16 years ago—it kicked off a mobile app revolution. Since then, mobile apps have become an indispensable part of daily life. Americans downloaded more than 12 billion apps each year between 2019 and 2021.[1] According to 2017 and early 2018 reporting,[2] the average smartphone user has more than 80 apps installed, uses nine or ten apps per day, and uses 40 apps per month. As of 2021, the average United States smartphone user spends more than four hours on apps every day—*more than a quarter of their waking lives*.[3] As people spend more and more time on mobile apps,[4] those spaces have grown infested with code that tracks their every move and monetizes their data.

2. Much of that code belongs to Google, the dominant mobile app advertiser and collector of mobile app activity data in the United States. Through "software development kits" (SDKs), Google has spread its code to virtually every person's phone, with Google tracking and saving vast volumes of information from hundreds of millions of Americans' app activity. On Android, more than 80% of the top 1,000 apps contain the Google Mobile Ads (GMA) SDK, which supports Google AdMob and Google Ad Manager.[5] Google AdMob is also "the most popular [SDK] for

---

[1] *Number of Mobile App Downloads Worldwide From 2019 to 2021 By Country*, Statista, https://www.statista.com/statistics/1287159/app-downloads-by-country/ (Last accessed February 15, 2023).

[2] *Spotlight on Consumer App Usage: Part 1*, App Annie, http://files.appannie.com.s3.amazonaws.com/reports/1705_Report_Consumer_App_Usage_EN.pdf (Last accessed March 17, 2023); Lexi Sydow & Sam Cheney, *2017 Retrospective: A Monumental Year for the App Economy*, App Annie, https://www.data.ai/en/insights/market-data/app-annie-2017-retrospective/#download (Last accessed March 17, 2023).

[3] Donny Kristianto, *Wining the Attention War*, data.ai, https://www.data.ai/en/insights/market-data/q1-2021-market-index (Last accessed March 17, 2023).

[4] Nick G., *55+ Jaw Dropping App Usage Statistics in 2023*, Techjury, https://techjury.net/blog/app-usage-statistics/#gref (Last accessed March 17, 2023) (Mobile users spend 87% of their usage time in apps).

[5] "GMA SDK can be used for both Google Ad Manager and AdMob ads." *Overview of Apps With Ad Manager*, Google, https://support.google.com/admanager/answer/6238688 (Last accessed February 15, 2023); Google AdMob, https://admob.google.com/home/ (Last accessed February 15, 2023); "Among Android apps, Google Ads AdMob was the most popular mobile ad network software development kit Google Ads AdMob Mediation Adapters was integrated with 88 percent of apps that used ad network SDKs." *Most Popular Installed Ad Network Software Development Kits (SDKs) Across Android Apps Worldwide as of March 2023*, Statista, https://www.statista.com/statistics/1035623/leading-mobile-app-ad-network-sdks-android/ (Last accessed March 17, 2023).

ads and monetization" on Apple products (iOS), "with roughly 80 percent integration reach" as of March 2023.[6] Google Analytics for Firebase (GA4F) is likewise integrated into millions of apps. By 2019, GA4F was included in 60% of the top apps, and that figure continued to grow (GOOG-RDGZ-00177433 at -452), such that over 1.5 *million* apps use Firebase each month.[7]

3. Google uses the Firebase and Google Mobile Ads SDKs to collect and save—for its own use and financial benefit—granular data regarding what people do not only Google apps (like Google Search and Google Maps) but also on non-Google apps, including, for example, E*Trade, Facebook, Glassdoor, GoodRx, LinkedIn, Lyft, Paypal, the New York Times, Uber, Walmart, Venmo, Yahoo Mail, and Zillow (all of which use Firebase). As a result, Google is able to uniformly and systematically collect and save data regarding where users click, forms they fill out, what they buy, and how they interact with ads.

4. Google has represented that users can control whether Google collects information about their app activity through a setting called "Web & App Activity" (WAA) and a sub-setting called "Supplemental Web & App Activity" (sWAA) (GOOG-RDGZ-00208190).[8] Google represents that WAA "must be on" "[t]o let Google save" information about your activity on "apps that use Google services," which include the Firebase and Google Mobile Ads SDKs.[9] Google employees including CEO Sundar Pichai have likewise touted how Google provides "clear toggles, by category, where [users] *can decide whether that information is collected* [and] *stored*."[10]

---

[6] *Most Popular Installed Ads and Monetization Software Development Kits (SDKs) Across iOS Apps in the Apple App Store Worldwide as of March 2023*, Statista, https://www.statista.com/statistics/1322629/top-apple-app-store-monetization-sdks/ (Last accessed March 17, 2023).
[7] Answer to Fourth Amended Complaint ("Answer") ¶ 231.
[8] *See infra* Section VII.J.
[9] GOOG-RDGZ-00000120.
[10] Sarah Perez, "*Google's CEO Thinks Android Users Know How Much Their Phones Are Tracking Them*," TechCrunch, https://techcrunch.com/2018/12/11/google-ceo-sundar-pichai-thinks-android-users-know-how-much-their-phones-are-tracking-them (Last accessed March 17, 2023) (emphasis added); *see also Google CEO Sundar Pichai Questioned on Tracking of Users' Location*, YouTube, https://www.youtube.com/watch?v=iv2BeDqxTEA (Last accessed March 17, 2023).

5. As I explain in detail in this report, the WAA and sWAA settings are privacy theater[11]; they do not function as described. Throughout the class period,[12] and uniformly for all class members, Google has continued to collect and save app activity data even when users have turned off WAA or sWAA. These users have these settings "off," and yet Google has continued to collect and save their app activity data. In my review of WAA- and sWAA-off data produced from Google's logs, I also found many unique Google identifiers that link this data to users—including name, email and address, phone number, and device identifiers—thus revealing users' most private app activity. Yet, Google does not even show users this data, or provide any way for users to delete it. Nor does Google provide any control whereby users or developers can stop Google from collecting and saving this data. To top it off, Google saves this WAA- and sWAA-off data (collected via the Firebase and Google Mobile Ads SDKs) in so many places, and uses it in so many ways, that even Google seems to have lost track.

6. There can be no legitimate dispute that Google saves and uses this WAA- and sWAA-off data to enrich itself. Google uses it to serve advertisements, to charge advertisers for those advertisements, and to test the effectiveness of those advertisements, which in turn enables Google to make more money. Google also uses this WAA- and sWAA-off data to train Google's machine-learning algorithms and to run experiments about the impact of potential changes to Google products and services, all of which allow Google to obtain new customers and charge more for its services. The trove of data Google collects from its users provides Google with significant competitive advantages over its competitors.

[11] "Privacy theater" is described as something "marketed as a step forward for consumer privacy, [that] does very little to change the underlying dynamics of an industry built on surveillance-based behavioral advertising." Gilad Edelman, *Google and the Age of Privacy Theater*, Wired, https://www.wired.com/story/google-floc-age-privacy-theater/ (Last accessed March 17, 2023)

[12] I understand from counsel that the class period in this case began on July 1, 2016 and continues through the present.

7. There is a better way. Google could change its processes so that switching off the WAA and sWAA toggles actually prevents Google from collecting and saving app activity data, as Google represented to users. Google could also purge its systems of WAA/sWAA-off data already collected, and delete any products, services, or algorithms built in whole or in part with WAA/sWAA-off data.

II. STATEMENT OF LIMITATIONS

8. This report has been prepared for purposes of this case only. It may not be used for any other purpose. This report contains and refers to information designated as "CONFIDENTIAL" and "HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY" under the Protective Order entered in this case, including information designated by both Plaintiffs and by Google.

III. ENGAGEMENT

9. Counsel for the Plaintiffs in this action ("Counsel") retained me to develop and render opinions concerning the technology and practices at issue in this litigation with respect to products developed and distributed by defendant Google, LLC ("Google"), based on my analysis and review of documents, testimony, written discovery, data produced,[13] and the testing described in this report. Specifically, I am focusing on Google tracking and advertising code through which Google collects mobile app activity during users' interactions with non-Google branded mobile apps. I am informed that the tracking and advertising code at issue in this case includes the Firebase SDK and Google Mobile Ads SDK, which supports AdMob, AdMob+, and Ad Manager. I am also focusing

[13] All documents considered appear in the attached Exhibit A.

on the WAA and sWAA settings that Google offers to accountholders. My report includes various appendices and exhibits, served with this main report.

10. I am being compensated for my work in this case at the rate of $800 per hour, which was my standard hourly rate as of the date of my engagement. My business partner, Julie Ann Burns, is charging $200 per hour, which was her standard hourly rate as of the date of her engagement. Our compensation does not depend upon the outcome of the case. I understand that, should there be any recovery in this case, Ms. Burns and I will be excluded from any disbursement of funds.

11. While I have used Firebase and the WAA activity control panel during the class period, before this engagement, I was not aware of Google's collection, storage, and use of WAA-off data. I only became aware through discovery in this case.

12. To the extent any other documents or data are produced or there is any further testimony or discovery, I reserve the right to supplement this report.

IV. EXPERTISE

13. I have a Bachelor of Science (BSc.) degree awarded *summa cum laude* and Master of Science (MSc.) degree in computer science, both from Yale University. I earned my degrees in 1990, one of four students in my class of 1500 to receive simultaneous degrees. My master's thesis, entitled *How to Create a Failure Tolerant Distributed System*, focused on distributed transaction processing and the distributed consensus problem. My coursework at Yale included theory of computation, distributed systems, artificial intelligence, systems programming, and operating systems. My thesis advisor was Dr. Michael J. Fischer, a renowned computer science professor known for his work in distributed computing. I was encouraged to attend Yale by, and then studied with, Dr. Alan Perlis, the first recipient of the Turing Award, the "Nobel Prize of computing."

14. Over the last 30 years I have maintained regular correspondence and meetings with my advisor, Dr. Fischer, which helps me to stay informed about the latest academic work in computer science. During the fall semester of 2020 I took his course CPSC 467: Cryptography and Security at Yale, and during the spring semester of 2021 I took his course CPSC 457: Sensitive Information in a Connected World.[14] The latter course placed a heavy emphasis on the ethical issues related to the handling of other people's data.

15. Dr. Fischer, Dr. Daniel Boffa, and I recently authored an academic paper, *Privacy-Preserving Data Sharing for Medical Research,*[15] that I presented at the 23rd International Symposium on Stabilization, Safety, and Security of Distributed Systems in November 2021. I also presented our work at the Yale Applied Cryptography Laboratory on October 22, 2021. This paper relates to the ethical handling of other people's sensitive data and computer security in general.

16. In 2022, I re-enrolled at Yale University as a PhD student in the Department of Computer Science. Yale provides me with a full scholarship and a stipend. I also serve as a Teaching Fellow and am part of the Yale Applied Cryptography Laboratory. My research specifically focused on identity and privacy.

17. I serve as an expert consultant and expert witness in the fields of software development; technology entrepreneurship; and Internet advertising, marketing, e-commerce, and security. A complete copy of my *curriculum vitae* is attached as **Appendix L.** It includes a list of prior cases in which I have testified as an expert at trial or deposition. As of the date of this report, I have

[14] Yale allows alumni to audit classes for a small fee.
[15] Michael J. Fischer, Jonathan E. Hochman, & Daniel Boffa, *Privacy-Preserving Data Sharing for Medical Research*, Yale University, https://cpsc.yale.edu/sites/default/files/files/TR1558.pdf (Last accessed March 17, 2023).

testified in twelve trials and at forty-seven depositions. I have been qualified as an expert by two US District Courts, four state courts, five arbitration tribunals and one District Court in Israel.

18. In total, as of the date of this report, I have spoken at thirty conferences across the country. In addition to speaking engagements, I have also published more than thirty articles as of the date of this report. A list of the articles I have published is included in my attached CV.

19. I am the founder of Hochman Consultants, an Internet marketing agency, established in 2004. Hochman Consultants provides clients with marketing strategy, website development, ecommerce, digital advertising, and Internet security services. Hochman Consultants also provides advice on search engine optimization and pay-per-click advertising, making websites more user friendly, increasing traffic, and increasing the value of each visitor.

20. In connection with my work at Hochman Consultants, for the past eighteen years, I have published short online articles, which address issues faced by my clients. In total, I have published eighteen of these articles, without funding by outside sources, as of the date of this report.

21. I am a member of the Association for Computing Machinery (ACM), the world's largest computing society, whose goal is to advance computing as a science and a profession. I am also a member of the Institute of Electrical and Electronics Engineers (IEEE), which describes itself as "the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity."

22. I am also a co-founder of the UNS Project, an Internet security venture to provide identity services, including user authentication and proof of unique personhood. UNS Project has built a high-security medical research data management system that has been deployed for testing by Yale New Haven Hospital, St. Mary's Hospital of Waterbury, Connecticut, and the Connecticut Tumor Registry.

23. I was a co-founder of CodeGuard, a startup information security company. In July 2018 CodeGuard was acquired by Sectigo, an information security company controlled by Francisco Partners, for an undisclosed price. CodeGuard had more than 250,000 paying customers as of 2018, when it was protecting more than 1 million websites and online databases from malicious attacks and accidental corruption. The CodeGuard product has since been integrated into the Sectigo Web Security Platform which is sold worldwide.

24. From 1999–2004, I served as a Director of Barcoding Inc., a systems integrator, which develops and provides software, mobile Applications, mobile computing, automatic data collection, and wireless networking. While I was a Director, Barcoding Inc. was named to the Inc. 500, recognized by Forbes Magazine as one of ten privately held companies to watch, and ranked third on the Maryland Fast 50. During my work at Barcoding Inc. I was responsible for the company's e-commerce platforms.

25. I presently hold Google Ads Search and Display Certifications. To obtain these certifications, I studied Google's training materials and passed Google's exams.[16]

26. I also hold a certification related to Biomedical Research, specifically because my research includes the design of software and protocols for handling sensitive patient data.[17]

27. I work for clients in numerous industries and government roles. My clients have included major corporations and organizations, such as Apple (on two occasions), Zillow, Delta Air Lines, U-Haul, the FDIC, and the US Treasury. My involvement has been disclosed in several significant class action litigations, including one that resulted in a $22.25 million proposed settlement by Yelp, one that resulted in a $187.5 million settlement by Snap Inc., and in *Brown v Google* where billions

[16] *Jonathan Hochman*, Skillshop, https://skillshop.credential.net/profile/jonathanhochman908080/wallet#gs.ta1wx3 (Last accessed March 21, 2023).
[17] *Jonathan Hochman*, Citi Program, https://www.citiprogram.org/verify/?wede459e0-804a-49bf-ad92-847cfe89b309-50611315 (Last accessed March 21, 2023).

in damages are claimed. I have written scores of expert reports, many of which are not reflected on my CV, because the cases settled prior to my testifying. In *Brown v Google*, I wrote an opening expert report and a rebuttal report, and Google neither challenged my qualifications nor sought to limit or exclude any portion of my opinions.

V. PREPARATION

28. I have had full access to every document produced in this case, using a document review platform provided by International Litigation Services ("ILS"), and to all deposition transcripts, written discovery responses, and data produced. I was freely allowed to conduct searches and view any document for the purpose of preparing this report, and my partner and I spent many hours independently searching for and reviewing documents produced in this case and reviewing the deposition transcripts, written discovery responses, and data and information produced.

29. I also reviewed public materials, such as Google support pages for the Google products at issue in this case.

30. I also reviewed developer interfaces of the Google Analytics for Firebase platform, including in connection with the test apps that I directed my consultants to develop (*see* Appendix I). My consultants and I conducted experiments with a web debugging and proxy tool called Fiddler Classic to assess the Google products at issue in this case.

31. For a two-week period in January 2023, I worked with my consulting experts to conduct tests to observe data traffic sent to Google and stored in Google logs. Google produced some of the data that was generated through this process, and my consultants and I reviewed and analyzed that data. Google limited this data production process to a small number of analytics and ads logs, while refusing to provide the log schema and field descriptions for the produced data.

32. I have supervised the following consulting experts to assist me in the preparation of this report: Mr. Jay Bhatia, Dr. Lillian Dai, Mr. Vivek Shinde, Mr. Jake Taylor, Mr. Christopher Thompson, various engineers employed by Concur IP, and Ms. Julie Ann Burns. With the assistance of the consulting experts under my direction and guidance, I have analyzed data traffic from Android and iOS devices and installed apps.

33. I have also had conversations with Mr. Michael Lasinski (Plaintiffs' damages expert) and members of his team.

34. All opinions rendered in this report are my own.

VI. BACKGROUND

35. For purposes of my analysis and opinions, I assumed the following:

1) The operative complaint is the Fourth Amended Complaint.

2) The relevant period started on July 1, 2016, and is ongoing (the "class period").

3) Plaintiffs allege two classes:

- Class 1 – All individuals who during the Class Period (a) turned off "Web & App Activity," or supplemental "Web & App Activity," and (b) whose mobile app activity was still transmitted to Google, from (c) a mobile device running the Android operating system (OS), because of the Firebase SDK and/or AdMob SDKs, on a non-Google branded mobile app.

- Class 2 – All individuals who during the Class Period (a) turned off "Web & App Activity," or "supplemental Web & App Activity," and (b) whose mobile app activity was still transmitted to Google, from (c) a mobile device running a non-Android operating system (OS), because of Firebase SDK and/or AdMob SDKs, on a non-Google branded mobile app.

36. I will first provide a high-level overview of some of the key technologies and topics pertinent to this case.

A. Google Accounts

37. I understand from Counsel that this case pertains to Google account holders in the United States. Since at least 2005, Google has offered Google accounts to people in the United States.[18] Although people commonly create a Google account by signing up for a Gmail email address, Google allows people to create a Google account associated with any email address.[19] Because all Gmail accounts are Google accounts but not all Google accounts are associated with Gmail accounts, the number of Google account holders in the United States will exceed the number of people in the United States who have at least one Gmail account.

38. Once a user obtains a Google account, Google associates the account with an internal ID called the GAIA (Google Account and ID Administration) ID[20] that is unique to that user account, along with the user's e-mail address, and if available, name, phone number, IP addresses and type of devices used over time, recovery e-mail/phone number and other information.[21] Google also saves a plethora of information related to Google account holders' app usage activities in Google servers as I will discuss in detail in this report. Google also saves a variety of other identifiers connected with a GAIA ID, including DSID (an encrypted form of the GAIA ID), device IDs (such as ADID on Android and IDFA on iOS devices), app instance id from Google Analytics for Firebase, and more.

---

[18] *Google Account Help*, Google, https://support.google.com/accounts/answer/27441 (Last accessed February15, 2023).
[19] Coleman, Keith, *"Sign Up for Gmail"*, Google Official Blog, https://googleblog.blogspot.com/2005/08/sign-up-for-gmail.html (Last accessed February 15, 2023).
[20] GAIA IDs were created in 2002. These IDs are used to identify "users signed in to Google services (e.g., search, Gmail)." GAIA IDs work "across devices, browsers, and mobile apps" and provide "Single Sign-On across Google services" (GOOG-RDGZ-00188195 at -207). Google sometimes refers to this ID as the "Google Account ID".
[21] Google provides a subset of information that it stores on Google account holders through a service called Google Takeout. Through discovery, I learned about voluminous other data that Google stores and which Google does not provide to Google account holders.

39. Google maintains several types of user accounts, including: consumer accounts (regular Google user accounts), enterprise user accounts (internally referred to as Dasher accounts whereby each user account is maintained by an enterprise administrator as well as the user), child accounts (internally referred to as Unicorn accounts for children under the age of 13 whereby each user account is managed by a parent) (GOOG-RDGZ-00130958 at -962; GOOG-RDGZ-00089523 at -523), and Googler accounts for Google employees (GOOG-RDGZ-00131873 at -875). Importantly, users who are students or employees may be required by their school or employer to have a Google account to use Google software that a school or employer utilizes, such as email. As a practical matter, a significant number of people have no real choice whether to have a Google account. They must have a Google account.

40. Google account holders sign into their Google account to access Google services (such as Gmail, Google Search, Google Photos, Google Maps, Google Drive, etc.). Google considers Android users "signed-in" if they are signed in at the device level (i.e., within the device's built-in Settings app) (GOOG-RDGZ-00200800 at -975). In addition, if an Android user signs in "anywhere on their phone (i.e., within one app), they are treated as signed in everywhere (across all apps)" (GOOG-RDGZ-00130015 at -034). For example, based on my testing on an Android phone, when a previously signed-out Android user signs into the Google Play Store app, they are automatically signed into that Google account in the Settings app and other Google apps on their device. Android users must be signed into a Google account to download an app from the Google Play Store. Users of iOS devices are treated as "signed in" to a Google account if they are signed in on any Google app on their device.[22] For example, if an iOS user is signed into the Gmail app,

[22] "For iOS, signed in means signed into a google app on the device" (GOOG-RDGZ-00200800 at -975).

then that user is considered "signed in" to Google for all purposes on that device.[23] In the rest of this report, unless I note otherwise, by "signed-in," I mean signed into a Google account.

B. Web & App Activity (WAA) and supplemental Web & App Activity (sWAA)

41. Web & App Activity (WAA) is a setting available in Google account holders' Google account settings. I understand that this case principally concerns data relating to activity on mobile applications, which run on mobile devices like smartphones and tablets. A few examples of well-known and widely used mobile apps include NYTimes, ESPN, Instagram, Reddit, and Netflix.

42. WAA is a parent setting to three child settings: (1) the Supplemental Web & App Activity (sWAA) setting, which Google also refers to as "Additional Web & App Activity" (GOOG-RDGZ-00088609); (2) the device-level sWAA setting, which Google refers to as "Supplemental Web & App Activity Device Level" (sWAAdl), that is available on some Android devices; and (3) an audio recording setting. My understanding is that this case is concerned with the WAA and sWAA settings.

43. The WAA setting relates to the user's activity on Google sites and apps, such as Google Search or Google Maps. The sWAA setting relates to activity on non-Google sites and apps that use Google services, such as the Firebase SDK or the Google Mobile Ads SDK. Because sWAA is a sub-setting of WAA, WAA also impacts activity on non-Google sites and apps.

44. Internally, Google refers to the WAA and sWAA settings (along with other Google account settings) as User Data Control (UDC) settings.[24] Users can access these settings either through Google account settings (under "Data & privacy" "History settings") or through the Settings app

[23] For iOS devices, Google employee Steve Ganem testified that "the user would be considered signed in if they - on an iOS device if they had installed one or more Google owned and operated apps and were signed in to one or more of those apps on that device" (Ganem Tr. 50:17-20).

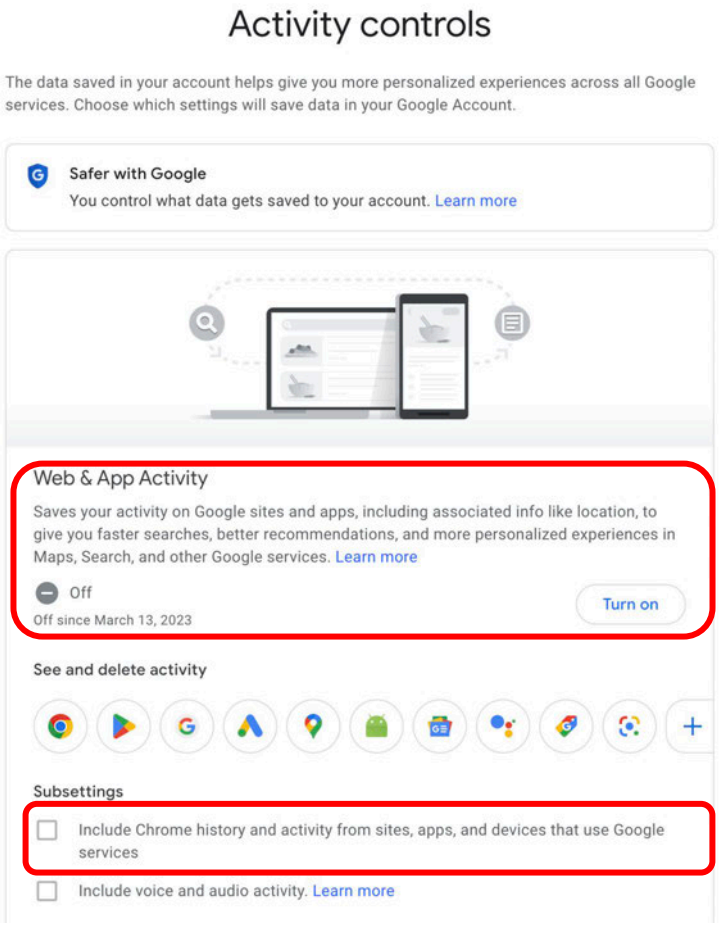
[24] According to Google's 30(b)(6) designee, David Monsees, "Both the UDC and activity controls are effectively the same" (Monsees Tr. 160:17-18). *See also* GOOG-RDGZ-00037220 at -222, -289 and -290.

on an Android device (within the "Privacy" section and "Activity Controls" subsection). During the class period, Google has presented the WAA setting as a toggle that can be switched on or off, or a button that users can "Turn on" or "Turn off." The child settings, including sWAA, are presented to users as boxes they can check or uncheck.

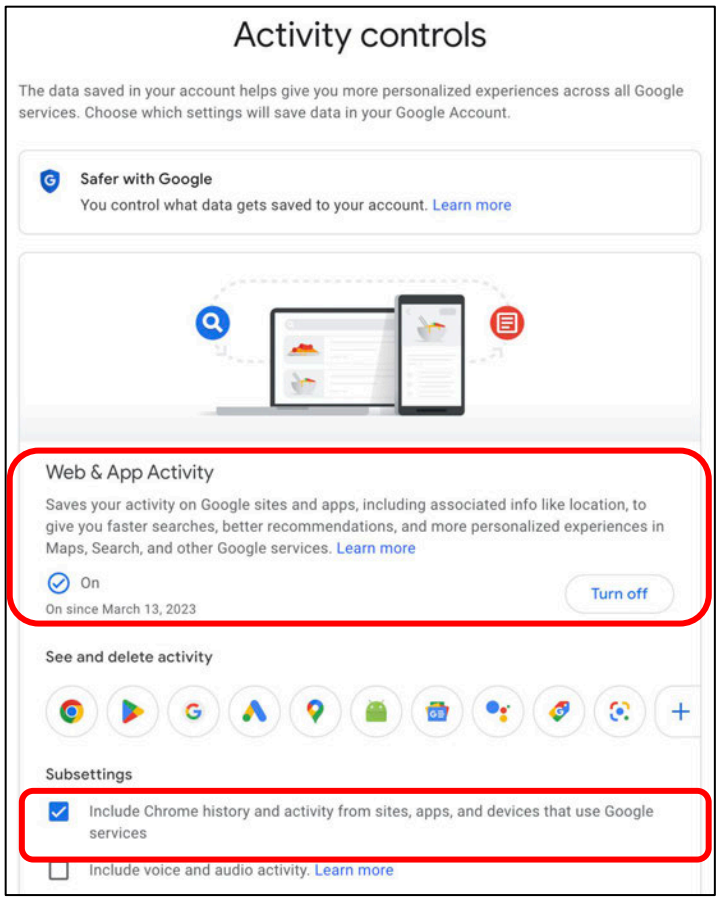
45. Below is a Figure showing how a user can access the WAA and sWAA settings from a desktop device,[25] as of March 13, 2023. In this figure, WAA and sWAA are both turned off. When WAA is turned off, an "Off" symbol shows under the Web & App Activity description and a button showing "Turn on" is available for the user to turn WAA on. When sWAA is turned off, the sWAA checkbox is unchecked.[26]

[25] This setting has the same user interface when accessed through an iOS device. Because these are account-level settings, a user who turns off WAA or sWAA while on a desktop also turns off WAA or sWAA on their mobile devices, provided those devices are signed into the same Google account.

[26] *Activity Controls*, Google, https://myactivity.google.com/activitycontrols (Last accessed March 19, 2023).

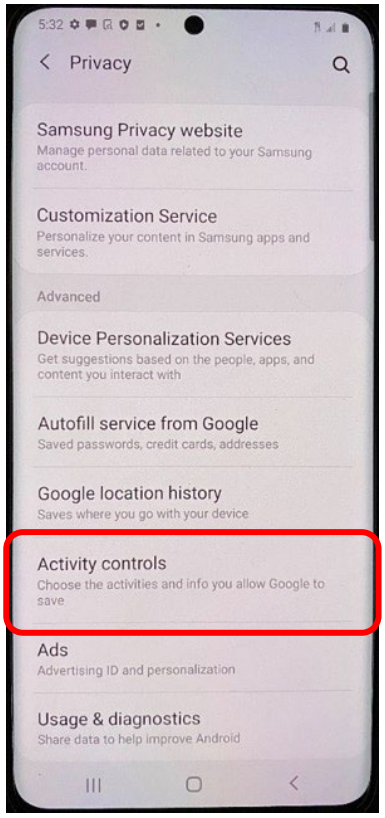


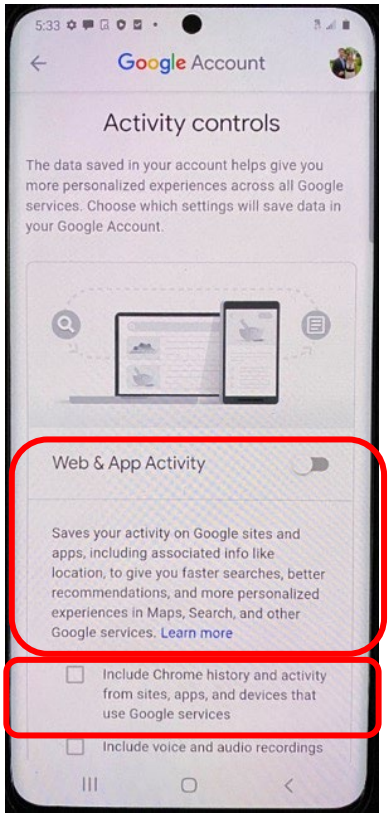
46. Below is a Figure showing both WAA and sWAA turned on. When WAA is turned on, an "On" symbol shows under the Web & App Activity description and a button showing "Turn off" is available for the user to turn WAA off. When sWAA is turned on, the sWAA checkbox shows a check mark. When WAA is turned on, the user can also turn sWAA off by unchecking the sWAA checkbox.

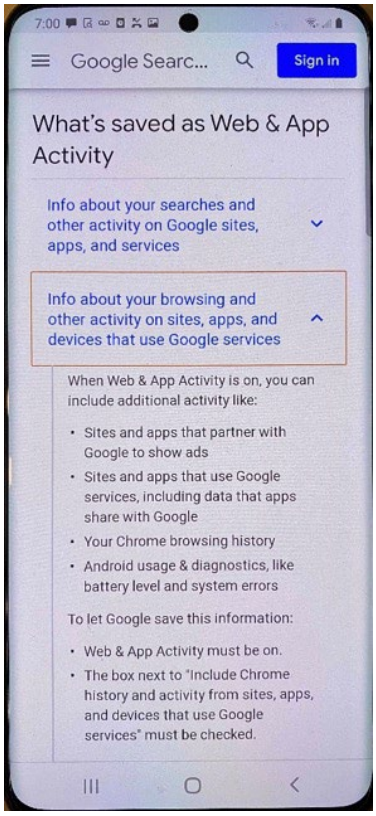


47. Below is a figure showing how a user can access the WAA and sWAA settings from an Android device as of July 2020. Screen 1 shows the Privacy options within the device Settings app, including "Activity controls," which Google presents as a page that allows the user to "[c]hoose the activities and info you all Google to save." When a user clicks on this option, Screen 2 appears, which contains the WAA and child settings, including sWAA. Here, the WAA setting is presented to the user as a slider and the sWAA setting is a checkbox. In Screen 2, both WAA and sWAA are turned off. A user can click on the "Learn more" link, which brings up Screen 3, containing a description of "What's saved as Web & App activity." Google has admitted in discovery that these device settings on the Android operating system were designed and drafted

by Google.[27] This shows that Google presents the Activity controls on Android devices as device setting controls.



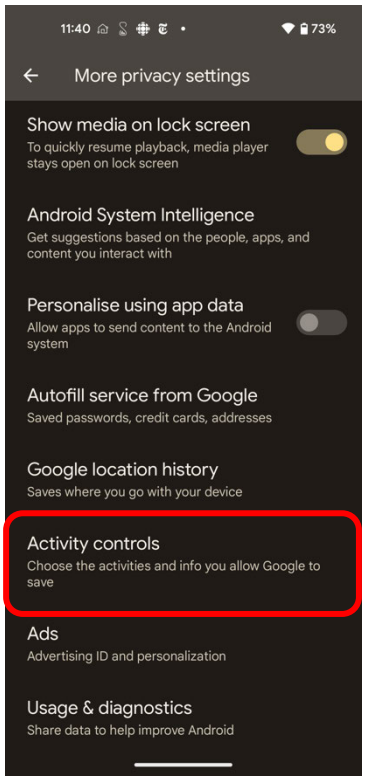




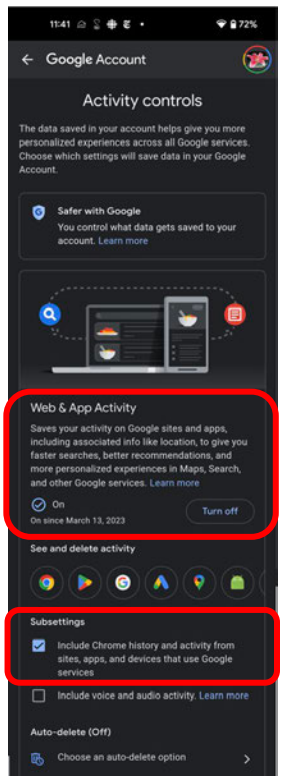
SCREEN 1 SCREEN 2 SCREEN 3

48. Google has since updated this interface. Below is a figure showing how a user can access the WAA and sWAA settings from an Android Google Pixel device as of March 13, 2023. Screen 1 shows the "More privacy settings" options within the device Settings app, including "Activity controls." Screen 2 shows the current "Activity controls" page with the same user interface as I showed earlier in the desktop version of the Activity controls page. Screen 3 shows the "Learn more" page.

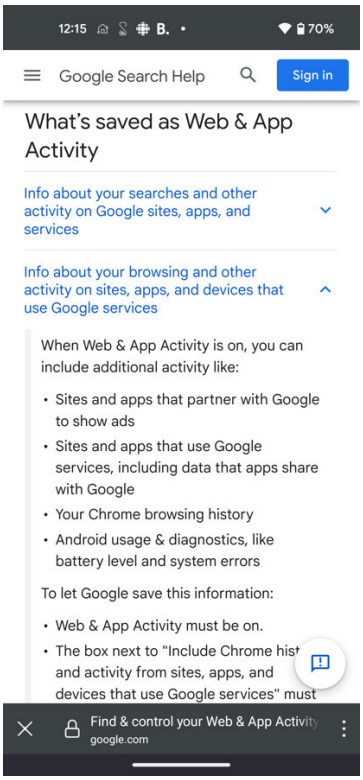
[27] The text on Screens 1 and 2 is the same as the text displayed on Google's own webpages. Google's counsel confirmed that the text associated with the "Activity controls" page on Screen 1 was drafted and controlled by Google throughout the class period. Email of E. Santacana, "RE: Rodriguez v. Google: OEM Communications" (Oct. 29, 2022).



SCREEN 1



SCREEN 2



SCREEN 3

49. On both Android and iOS devices, the WAA and sWAA settings can also be accessed through Google apps (e.g., Gmail), through a "Manage your Google Account" button associated with the signed-in Google account.

50. When WAA is turned on, sWAA can be turned either on or off. When WAA is turned off (or, equivalently, disabled or paused), sWAA is turned off automatically and cannot be turned back on (unless WAA is first turned back on).[28] WAA and sWAA are account settings that can be turned on or off across multiple devices.[29] In other words, a user's WAA and sWAA statuses are applied

[28] Former Google employee Greg Fair testified that "sWAA is a subsetting of WAA. If you turn off WAA, sWAA also turns off" (Fair Tr. 187:7-9). "Q. can sWAA be enabled with WAA being disabled? A. No" (Fair Tr. 189:10-12). *See also* GOOG-RDGZ-00018661 at -662 ("SWAA is a child setting of 'Web & App Activity' (WAA). WAA must be on for SWAA to be turned on."); Answer ¶ 78 ("[A] user can elect to turn Web & App Activity on or pause the feature, and when Web & App Activity is on, users can elect to turn supplemental Web & App Activity on or pause the feature.").

[29] "Web & App Activity and supplemental Web & App Activity are account settings that can be turned on or paused across multiple devices" (Answer ¶ 80).

across all devices on which the user is signed-in to the same Google account. As discussed earlier, Google presents WAA and sWAA controls as both account setting controls and device setting controls.

51. WAA and sWAA states are "sticky," meaning it is unlikely for users to frequently change the setting state. According to an internal 2018 Google document, "[redacted] (GOOG-RDGZ-00209874 at -875). A Google engineer says in an internal e-mail, "Yes, the fact that WAA is a pause control may be relevant from a theoretical/philosophical perspective, but most users probably use it as a permanent opt-out/opt-in control, instead of toggling" (GOOG-RDGZ-00209764 at -765).

52. The predecessor to WAA was called "Search History," "Google Web History," or "Show My History" (SMH).[30] The Search History and Google Web History settings were initially launched in 2005 (GOOG-RDGZ-00037220 at -289). According to an Internet archive of Google's Help webpage for Google Web History, dated March 20, 2013,[31] Google Web History was automatically turned on when a user created a Google account, and it made visible to users information related to Google search queries, search results, and the URLs of webpages visited. When Google Web History (alternately referred to as Show My History (SMH)) was turned on,

[30] GOOG-RDGZ-00018661 at -662 ("WAA is the current iteration of the setting variously known as 'Search History' and 'Web History' in the past; it is the generalized mechanism for controlling cross-product sharing of activity data across Google services."); GOOG-RDGZ-00035990 at -990 ("WAA: Web & App Activity, f.k.a., search history, web history, show my history showmyhistory: name of WAA service.").

[31] Google Inside Search, https://web.archive.org/web/20130405085716/http://support.google.com/websearch/answer/54068# (Last accessed February 15, 2023).

user data was processed via an internal Google system called Footprints, and the data was stored in a Google storage system called Kansas (GOOG-RDGZ-00035691 at -701 and -706).[32]

53. In 2014, Google introduced the Supplemental Web and App Activity (sWAA) control "as part of a major revamp of [their] Activity Controls (UDC)" (GOOG-RDGZ-00204257 at -328). In early 2015, Google renamed "Search History" and "Google Web History" to "Web & App Activity" (WAA),[33] and bundled that new control with another that offered users the choice to "include history from Chrome and other apps in your Web & App Activity," which Google internally called "supplemental Web & App Activity" (sWAA) or alternatively "Additional Web & App Activity" (GOOG-RDGZ-00088609; GOOG-RDGZ-00204257 at -328).

54. In mid-2016, Google began a multiyear overhaul of their Display Ads system[34] to enable Google to associate user data from non-Google apps and websites with users' GAIA IDs. When Google acquired an internet advertising company called DoubleClick in 2008, it promised regulators that it would maintain the so-called pseudonymity of data associated with display ads.[35] Accordingly, Google designed its display ads architecture not to link GAIA ID to data associated with display ads. But this design decision was costly. By linking users' data to their GAIA ID, Google could better track users across apps and websites, on any device, and even when other identifiers may not be available. By connecting users' data relating to activity on both Google and

[32] "Kansas is a data storage infrastructure within Google that the Footprints infrastructure utilizes" (Monsees Tr. 114:7-9). In addition to Kansas, "Footprints supports various data storage infrastructure within Google" such as Spanner and [redacted] (Monsees Tr. 115:6-7, 115:11-12, 115:15-19).

[33] *Google's Web & App Activity*, Google Operating System, https://googlesystem.blogspot.com/2015/01/googles-web-app-activity.html (Last accessed February 15, 2023).

[34] Google's advertisement infrastructure broadly includes Display Ads for ads served on non-Google publisher websites and apps as well as on Google properties such as Gmail and Google Play; Search Ads for ads served on Google.com, Google search apps and Google search partner properties; and YouTube Ads for ads embedded in YouTube videos (GOOG-RDGZ-00014026 at -026).

[35] "Even if you are signed in to Google, the activities you do on Google sites, remain separate from the activities you do on non-Google sites and for every device or cookie jar you use, we see you as a separate identity.. . . In 2008, Google added similar language to its Privacy Policy as part of the regulatory approval process for the purchase of Doubleclick" (GOOG-RDGZ-00183010 at -023).

non-Google properties, Google can maintain a more complete view of the user, and thereby generate more advertising revenue. In mid-2016, Google began efforts to link those datasets notwithstanding its promises to regulators in 2008. This effort was codenamed "Narnia 2.0," [redacted]

55. Broadly speaking, Narnia 2.0 [redacted] which allowed ads personalization. Google's objective was threefold: "Maximize user's perception of Google with respect to trust and privacy," "Maximize the number of users who knowingly accept the invitation to update their account to the new default state," and "Maximize comprehension of the change, based on the user's ability and desire for detail" (GOOG-RDGZ-00018661 at -662 and -663). Publicly, Google told users that the purpose of this effort was to enable new features, giving users "more control over the data Google collects and how it's used, while allowing Google to show you more relevant ads" (GOOG-RDGZ-00164315 at -329 and -330; See full text below this paragraph).[36] As can be seen below, Google promised users that "You control the types of information we collect and use at My Account"; however, Google did not inform users that they have no control over the shadow account where Google stores data even if users do not turn WAA or sWAA on.

[36] Google pushed what they called a "Consent Bump" to both new and existing Google account holders in an effort to entice them to enable sWAA and NAC (GOOG-RDGZ-00018661 at -673). [redacted] Monsees Tr. 52:16-53:10).

Some new features for your Google Account

We've introduced some optional features for your account, giving you more control over the data Google collects and how it's used, while allowing Google to show you more relevant ads.

What changes if you turn on these new features?

- **More information will be available in your Google Account, making it easier for you to review and control:** When you use Google services like Search and YouTube, you generate data — things like what you've searched for and videos you've watched. You can find and control that data in My Account under the *Web & App Activity* setting. With this change, this setting may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.

  <If Chrome Sync is enabled>*You have Chrome browsing history stored in your Google Account. Learn more about how turning on this setting affects how this data is used for personalization.*

- **Google will use this information to make ads across the web more relevant for you:** In My Account, the Ads Personalization setting currently lets Google use data in your account to tailor ads that appear in Google products. With this change, this setting will also let Google use data in your account to improve the relevance of ads on websites and apps that partner with Google.

These settings apply across all of your signed-in devices and across all Google services. You can change them any time in My Account. Learn more <Link to "Learn More" content> about these features, including how they affect shared devices.

What's still the same?

- Google does not sell your personal information to anyone
- You control the types of information we collect and use at My Account (myaccount.google.com)

Choose I AGREE to turn these features on or MORE OPTIONS for more choices.

MORE OPTIONS | I AGREE

56. Around the same time, Google released a new My Activity page where users who have WAA or sWAA enabled can see some of their web and app activity data.[37] As an online article at the time explained, "the main difference between the My Activity page and the former Web History tool is that My Activity shows activity from a variety of Google's products, not just Search, Image Search and Video Search."[38] According to documents Google produced in this litigation, Google understood My Activity as "the tentpole user trust feature for the Narnia 2.0 launch"

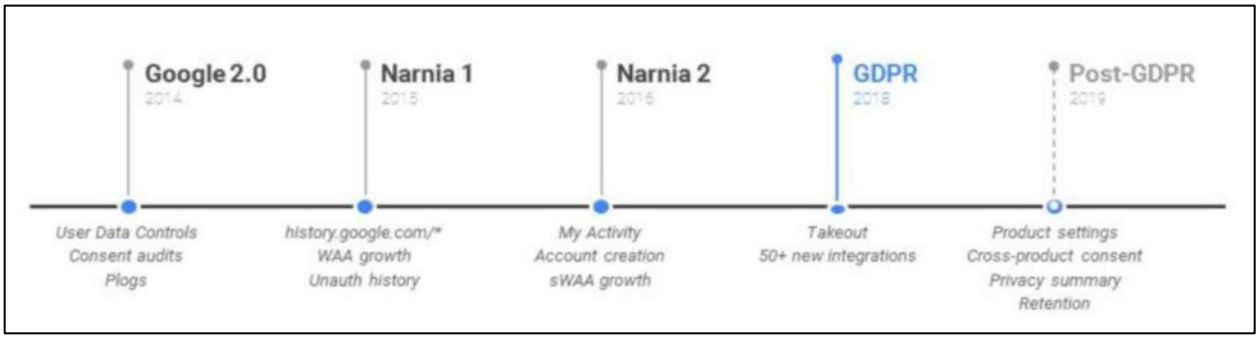
[37] GOOG-RDGZ-00013908 (details regarding the launch of the My Activity page); GOOG-RDGZ-00019095 at -100 (Monsees, stating that "The Narnia 2.0 effort would not have been possible without my timely and successful landing of the My Activity product.").

[38] Sarah J. Purewal, *Everything You Need To Know About Google's My Activity Page*, Cnet, https://www.cnet.com/tech/services-and-software/everything-you-need-to-know-about-googles-my-activity-page/ (Last accessed February 15, 2023).

(GOOG-RDGZ-00019095 at -099). Because of My Activity, Google was able to focus press and regulator attention "on the transparency improvements" and convince them that Narnia 2.0 "was a privacy positive change," notwithstanding the changes to the way Google collected and stored user data (GOOG-RDGZ-00019095 at -099 and -100).

57. In connection with Narnia 2.0, Google also changed default settings for new Google accounts. Initially, sWAA was turned off by default for new Google accounts. In mid-2016, in connection with Narnia 2.0, Google reversed course; for any new Google accounts, sWAA would thereafter be turned on by default.[39]

58. A timeline of Google's WAA and sWAA controls is shown reproduced in the Figure below (GOOG-RDGZ-00018455 at -457).



C. Firebase

59. Firebase, also referred to as the Google Mobile Platform (GMP), is Google's app development platform that is widely used and integrated into many mobile apps (GOOG-RDGZ-00056947 at -947 and -954). It is one of the primary ways that Google collects data through non-Google mobile applications, and it is one of Google's main mobile application products. In 2020,

[39] GOOG-RDGZ-00188725 at -730 ("Today, sWAA is OFF per default. Post-Narnia 2.0, sWAA will be ON by default after the user has accepted the [redacted] consent and can be toggled as part of that consent flow."); GOOG-RDGZ-00020690 ("sWAA is on by default for all new gaia as of July 2016, that's another driver of growth."); GOOG-RDGZ-00037934 ("sWAA has only been on by default since [redacted] launch."); GOOG-RDGZ-00145258 ("sWAA was off by default from 2014 when it was introduced until mid 2016 when Narnia 2.0 came along."); GOOG-RDGZ-00023187 at -188 ("sWAA launched in 2014 and became an opt-out setting in July 2016.").

Firebase was used in 97% of the top one thousand apps on Android and 54% of top one thousand apps on iOS (GOOG-RDGZ-00060716 at -729).

60. Firebase was originally a startup founded in 2011 that provided an app development platform and hosting service for app developers. Google acquired Firebase in October 2014.[40] Google then launched Firebase as a Google product in May 2016.[41] According to Google, "Firebase … seamlessly integrates Google's cross-platform tools and services … on one SDK,[42] with free analytics at its core" (GOOG-RDGZ-00195309 at -341). At the time Google launched Firebase as a Google product, Firebase contained 15 products, including Analytics, App Indexing, Dynamic Links, AdWords and AdMob (GOOG-RDGZ-00195309 at -342).

61. While Google's public position on Firebase is that it "makes it very easy for developers to build mobile and web apps that store and sync data in real time,"[43] Google's internal documentation reveals that "Firebase is strategically critical for Google's long-term success" (GOOG-RDGZ-00070574 at -575). Firebase's "strategic value for Google, is much bigger than just helping developers build apps" (GOOG-RDGZ-00056947 at -956). Firebase "matters to

[40] Frederic Lardinois, *Google Acquires Firebase To Help Developers Build Better Real-Time Apps*, TechCrunch, https://techcrunch.com/2014/10/21/google-acquires-firebase-to-help-developers-build-better-realtime-Apps/ (Last accessed February 15, 2023).

[41] "Firebase is Google's app development platform, just launched in May. It seamlessly integrates Google's cross-platform tools and services along the game lifecycle, on one SDK, with free analytics at its core" (GOOG-RDGZ-00195309 at -341).

[42] "SDK stands for Software Development Kit" (GOOG-RDGZ-00056514 at -514). As Google explains, "SDK or "Software Development Kit" is a group of tools, including pieces of code, that are embedded into a service (in this case, an app). The SDK contains one or multiple APIs [Application Programming Interfaces] and so, the SDK calls on the API(s) to perform different functions. SDKs allow apps to integrate a lot of services including: ad monetization products, attribution partners, analytics, push notifications, crash analytics, etc." (GOOG-RDGZ-00030109 at -118). In Google's Answer to Plaintiff's Fourth Amended Complaint, "Google admits that Firebase SDK is a suite of software development tools intended for use by app developers" and "Google admits that as used in the phrase 'Firebase SDK,' SDK stands for 'software development kit'" (Answer ¶ 39).

[43] *Welcome Firebase to the Google Cloud Platform Team,* Google Cloud Platform Blog, https://cloudplatform.googleblog.com/2014/10/welcome-firebase-to-google-cloud-platform.html (Last accessed February 15, 2023).

Google" because, among other things, it "[b]oosts downstream business opportunities," in "Ads, Play, Cloud and more" (GOOG-RDGZ-00056947 at -956).[44]

62. As mentioned above, one of the products in the Firebase suite is an analytics product, which was initially released as Firebase Analytics and was rebranded as Google Analytics for Firebase (GA4F) in May 2017 (GOOG-RDGZ-00059723 at -723; GOOG-RDGZ-00057998 at -999; Ganem Tr. 18:11-15, 106:12-14). GA4F is an app measurement tool, which collects data relating to user activity on apps. To use GA4F, app developers must embed the Firebase SDK code into their apps. Google internally refers to its app measurement efforts, including GA4F, by the codename "Scion."[45] GA4F adoption is important to Google, as it allows Google to collect and save "high-fidelity signals to power Ads ML [machine learning]" technology (GOOG-RDGZ-00177709 at -711). GA4F "is the most-used analytics SDK on Android, in use by over 1.2M apps, including many large 3P [non-Google owned] and 1P [Google owned] apps" (GOOG-RDGZ-00050615 at -615).

63. For app developers who use Firebase, GA4F is enabled by default (GOOG-RDGZ-00092368 at -372). Google recognizes that "full functionality across the services *requires* our analytics to be on" (GOOG-RDGZ-00092368 at -372). GA4F "is tightly integrated with Ads," and "shares a developer's analytics data to enhance our advertising services" by default (GOOG-RDGZ-00092368 at -372).

[44] Google ads refers to Google's advertising business, including serving advertisements in mobile apps as well as ad performance tracking. Google derives most of its hundreds of billions of annual revenue from its advertising business. *Form 10-K*, https://www.sec.gov/Archives/edgar/data/1652044/000165204422000019/goog-20211231.htm (Last accessed March 17, 2013). Google Play refers to Google's Play App Store through which users can download and install apps on Android devices. Google charges developers a service fee as a percentage of their earnings related to app purchases. *Play Console Help*, Google, https://support.google.com/googleplay/android-developer/answer/11131145?hl=en (Last accessed March 17, 2023). Google Cloud offers hosting, data storage and data analysis services with a pay-as-you-go fee structure. *Google Cloud*, Google, https://cloud.google.com (Last accessed March 17, 2023).

[45] GOOG-RDGZ-00051774 at -776; Ganem Tr. 106:9-11 ("Scion is an internal code name that is associated with our app measurement efforts in Google Analytics.").

64. Internally, Google pushed to unify web and app analytics via a project codenamed "[redacted]" According to documents Google produced in this case, "[t]he web side of Google Analytics was also showing its age, so [Google] knew [Google would] need a more durable technology stack to carry the product into the future. This spawned 'Project [redacted]' to build GA4. It was originally called '[redacted] or '[redacted],' the atomic symbol for gold. [Google's] goal was to bring app and web analytics together, and to do it at a scale sufficient for [their] largest customers." (GOOG-RDGZ-00123526 at -526 and -527). "In the summer of 2019, [Google] launched the app and web beta, also known as [redacted] which introduced the new Google Analytics to web and hybrid customers" (GOOG-RDGZ-00123526 at -526 and -527). Google now had "cross-platform data come together for the first time in a common data model" (GOOG-RDGZ-00123526 at -526 and -527). Around this time, Google launched a beta version of Google Analytics 4 (GA4).[46] As Google explained in documents produced in this litigation, GA4 was a completely new analytics product only from a web perspective; it was "based on the Google Analytics for Firebase" platform, meaning that Google "mov[ed] [its] Web Analytics onto the Firebase Analytics back-end." Apps did not have to migrate to join GA4 (GOOG-RDGZ-00034472 at -475). GA4 included "features like native integrations, privacy capabilities and machine learning to automatically analyze data" (GOOG-RDGZ-00123526 at -526 and -527). GA4 fully launched in October of 2020.[47] In this report, when I refer to GA4F, I include GA4 (limited to its inclusion in apps) as it is the next generation of GA4F.

[46] Vidhya Srinivasan, *Introducing the New Google Analytics*, Google Marketing Platform, https://blog.google/products/marketingplatform/analytics/new_google_analytics/ (Last accessed March 9, 2023); GOOG-RDGZ-00123526 at -526 and -527.
[47] Vidhya Srinivasan, *Introducing the New Google Analytics*, Google Marketing Platform, https://blog.google/products/marketingplatform/analytics/new_google_analytics/ (Last accessed March 9, 2023).

65. Aside from Analytics, Google Firebase includes several other features, including Predictions, App Indexing[48], Dynamic Links, Cloud Messaging, among many others as shown in the figure below (GOOG-RDGZ-00060716 at -728).

66. Firebase Cloud Messaging enables app developers to send messages and notifications to users. It is integrated with Analytics and Predictions to target such messages "based on user actions (past, present, and future) and interests" (GOOG-RDGZ-00060716 at -757). Firebase Cloud Messaging (FCM)'s predecessor was called Google Cloud Messaging (GCM), which was launched in 2012 for Android devices and 2015 for iOS devices.[49] With the launch of Firebase in

[48] Firebase App Indexing, formerly known as Google App Indexing, was launched in 2016. Since January 2021, Google no longer recommends its use. Instead, Google recommends Android App Links and Universal Links as ways to link users from search results, websites and other apps to specific content within apps. Laurence Moroney, *Introducing Firebase App Indexing*, The Firebase Blog, https://firebase.blog/posts/2016/06/introducing-firebase-app-indexing (Last accessed February 15, 2023); *Firebase App Indexing*, Google, https://firebase.google.com/docs/app-indexing (Last accessed February 15, 2023). *See also* GOOG-RDGZ-00080040 at -046; GOOG-RDGZ-00080071 at -085 (App Indexing deprecation date).

[49] Angana Ghosh, *Introducing 4.1 (Jelly Bean) Preview Platform, and More*, Android Developers Blog, https://android-developers.googleblog.com/2012/06/introducing-android-41-jelly-bean.html (Last accessed February 15, 2023); Jon Fingas, *Google's Cloud Messaging Now Sends Notifications to iOS Devices*, Engadget, https://www.engadget.com/2015-05-28-google-cloud-messaging-on-ios.html (Last accessed February 15, 2023).

2016, Google rebranded Google Cloud Messaging to Firebase Cloud Messaging (FCM) (GOOG-RDGZ-00092368 at -372). GCM was deprecated in 2019 (GOOG-RDGZ-00123883 at -883).

67. Firebase Predictions applies Google's machine learning algorithm to app analytics data to predict things such as "user segments likely to churn, to spend, or to complete another custom conversion event" (GOOG-RDGZ-00060716 at -759). These functionalities are "integrated with Push Notifications, In-App Messaging, and Remote Config" (GOOG-RDGZ-00060716 at -759).

68. Firebase Dynamic Links (FDL) are HTTPS URLs that link into specific app content. According to documents Google produced in this litigation, "FDL ensures deeplinks survive app installs" (GOOG-RDGZ-00124287 at -289). While Android App Links and iOS Universal Links are technologies that can deep-link into mobile apps when the app is already installed, FDL links a user to an app whether it is installed or not (GOOG-RDGZ-00124287 at -289). When the app is not installed, the user is taken to the app store to download the app. In addition, FDL provides analytics information "such as clicks, first-opens, and re-open" and can be integrated with Google Analytics (GOOG-RDGZ-00124287 at -290).

D. AdMob SDKs

69. Just as Google built its mobile app development and analytics capabilities through the acquisition of Firebase, Google built its mobile app advertising business through its acquisition of AdMob. AdMob was originally a startup founded in 2006 and was acquired by Google in May of 2010.[50] As Google explained at the time of the acquisition, "AdMob was one of the first companies to serve ads inside mobile applications on the Android and iPhone platforms."[51] Before it acquired AdMob, Google did not have significant presence in the mobile app advertising market; its only

[50] *We've Officially Acquired AdMob!*, Google Official Blog, https://googleblog.blogspot.com/2010/05/weve-officially-acquired-admob.html (Last accessed February 15, 2023).
[51] *We've Officially Acquired AdMob!*, Google Official Blog, https://googleblog.blogspot.com/2010/05/weve-officially-acquired-admob.html (Last accessed February 15, 2023).

product was a beta version of AdSense for Mobile Applications (AFMA), which it launched in June of 2009.[52] Google migrated all customers using AdSense for Mobile Applications beta to AdMob in 2011.[53] From that point on, AdMob was Google's solution for serving ads within mobile apps, and AdSense was Google's solution for serving ads within websites.[54] AdMob became extremely popular. By 2016, AdMob was used in more than 1 million apps (GOOG-RDGZ-00195309 at -351).

70. According to documents that Google produced in this case, "AdMob is a full monetization platform" that "offers an industry-leading in-app ads network, mediation of dozens of other networks, a direct deals platform and cross-promo capabilities" (GOOG-RDGZ-00195309 at -350).

71. In order to use AdMob, app developers must embed the Google Mobile Ads (GMA) SDK in their apps.[55] The Google Mobile Ads SDK also supports Google Ad Manager (abbreviated GAM, alternatively called Display Reservation Exchange (DRX)), which includes products previously known as DoubleClick for Publisher (DFP), and Ad Exchange (AdX).[56] Like AdMob, Google Ad Manager is a service that publishers can use to serve ads on their properties, but Ad

[52] *We've Officially Acquired AdMob!*, Google Official Blog, https://googleblog.blogspot.com/2009/06/announcing-adsense-for-mobile.html (Last accessed February 15, 2023).
[53] *AdMob is for Mobile App Developers. AdSense is for Mobile Web Publishers*, Google Mobile Ads Blog, http://googlemobileads.blogspot.com/2011/09/admob-is-for-mobile-app-developers.html (Last accessed February 15, 2023). Google has retained the name AFMA when describing the AdMob SDK, at least for a period of time (GOOG-RDGZ-00072642 at -643 (referring to the AdMob SDK also as afma-sdk)).
[54] *AdMob is for Mobile App Developers. AdSense is for Mobile Web Publishers*, Google Mobile Ads Blog, http://googlemobileads.blogspot.com/2011/09/admob-is-for-mobile-app-developers.html (Last accessed February 15, 2023).
[55] "Q. And here, it says 'GMA SDK' and then there's a diagram that has, you know, an arrow, Ad Request, and goes to AdMob or Ad Manager. Does that refresh your recollection about what the GMA SDK is? A. Yeah. I think that's an interchangeable term with the AdMob SDK" (Weng Tr. 59:6-12).
[56] GOOG-RDGZ-00073132 at -132 ("Google Mobile Ads SDK (AdMob, DFP, AdX): The Google Mobile Ads SDK is the latest generation in Google mobile advertising featuring refined ad formats and features, enabling developers to maximize their monetization on Android, iOS, and Windows Phone 8."); Sridhar Ramaswamy, *Introducing Simpler Brands and Solutions for Advertisers and Publishers*, Google The Keyword, https://blog.google/technology/ads/new-advertising-brands/ (Last accessed February 15, 2023) ("[W]e've been working to bring together DoubleClick for Publishers and DoubleClick Ad Exchange in a complete and unified programmatic platform under a new name–Google Ad Manager.").

Manager is marketed exclusively to "large publishers who have significant direct sales." Unlike AdMob, Google Ad Manager can serve ads on both mobile apps and the web (GOOG-RDGZ-00056936 at -936 and -937). According to documents Google produced in this case, two-thirds of the traffic on Google's app ads properties is attributable to AdMob, while the remaining one-third is attributable to Ad Manager (GOOG-RDGZ-00028472 at -473).

72. Beginning on May 18, 2016, Google integrated its AdMob and Firebase offerings.[57] A beta version of an integration between Ad Manager and Firebase was launched in 2021.[58] Each of these integrations was important to Google.[59] According to a Google employee, Google can use the data it collects and saves using AdMob and Firebase to give publishers "a better understanding of how … users and ads were performing inside their app" (Weng Tr. 63:11-15). As another Google employee puts it, "this integration aimed to give them a fuller picture of their monetization including ads revenue if this was part of their business model" (Ganem Tr. 87:7-14).

73. Fewer publishers than Google expected became early adopters of Google's integrated AdMob and Firebase solution.[60] According to documents Google produced in this litigation, many app developers that used AdMob were reluctant to use Firebase because doing so would require adding another SDK into their apps' code.[61]

---

[57] Internal Google Email on May 23, 2016: "We are thrilled to announce that we launched the AdMob/Firebase Linking Integration on 05/18! In this AdMob/Firebase integration, we introduce AdMob publishers to Firebase and the benefits of Firebase Analytics...Linking between AdMob and Firebase apps allows us to use data from Firebase Analytics to improve the AdMob experience and data from AdMob to improve the Firebase experience" (GOOG-RDGZ-00073583 at -583).

[58] June 14, 2021: "Link your Google Analytics 4 properties to Ad Manager to see integrated app data (Beta) You can now link your Google Analytics 4 (GA4) properties to your Ad Manager network with Firebase using the Admin settings in Ad Manager. Publishers must first add the Firebase SDK to their apps in order to link their GA4 property to their Ad Manager network." *Google Ad Manager Help,* Google, https://support.google.com/admanager/answer/10290437 (Last accessed February 15, 2023).

[59] GOOG-RDGZ-00058523 at -561 (integration between AdMob and Firebase was a "market differentiator").

[60] GOOG-RDGZ-00058360 at -361 ("the AdMob+Firebase integration only has 15% adoption.").

[61] GOOG-RDGZ-00060455 at -456 ("One of the main points of friction in the current AdMob/Firebase integration is the requirement to integrate multiple SDKs and sign-up for an additional product.").

74. To increase adoption of Google's combined ads and analytics solution, Google incorporated the core analytics code from Google Analytics for Firebase directly into the Google Mobile Ads SDK.[62] That way, Google could collect analytics data even in apps whose publishers do not use Firebase. Internally, Google called this new version of AdMob, "AdMob+." As explained in documents Google produced in this litigation, Google created AdMob+ "to ensure we are collecting analytics data for all AdMob publishers" (GOOG-RDGZ-00058360 at -361).

75. Google neither used the term "AdMob+" externally nor marketed its new capabilities as a separate product. Instead, in the summer of 2019 Google simply updated the existing Google Mobile Ads SDK, so that analytics functionality was automatically available.[63] According to documents Google produced in this litigation, Google aimed "to achieve 100% of analytics data collection for AdMob publishers," (GOOG-RDGZ-00076976 at -977) meaning that for all AdMob publishers, AdMob, just like GA4F would be "able to collect automatic events and user properties" (GOOG-RDGZ-00031656 at -656). The "AdMob+ SDK collects the same set of automatic signals as the GA4F SDK" (GOOG-RDGZ-00059486 at -486).

76. In this report, when I discuss the Google Mobile Ads (GMA) SDK, I am referring to its use for AdMob, AdMob+ and Ad Manager.

E. Mobile Apps and Webviews

77. It is helpful to distinguish between "web activity" in standalone web browsers (e.g., Chrome, Safari) and "app activity" other applications, which are often designed for a single

[62] GOOG-RDGZ-00076976 at -977 ("The Analytics SDK team has gone to great lengths to refactor our code so that the components and frameworks which are packaged with AdMob+ are generically branded ('AppMeasurement')."); GOOG-RDGZ-00060455 at -456 ("we will now merge the SDKs, forcing GMA to take a hard dependency on AppM, the core-measurement SDK. AppM will be a generic data collection SDK, which will reuse much of the existing [redacted] SDK code, and will strip all mentions of Firebase or FirebaseAnalytics."); *see also* GOOG-RDGZ-00067721 at -722.

[63] "In Summer 2019, as part of the AdMob+ project, AdMob updated their SDKs (iOS v7.44+ & Android v18.1.0+) to include measurement SDKs" (GOOG-RDGZ-00031656 at -656).

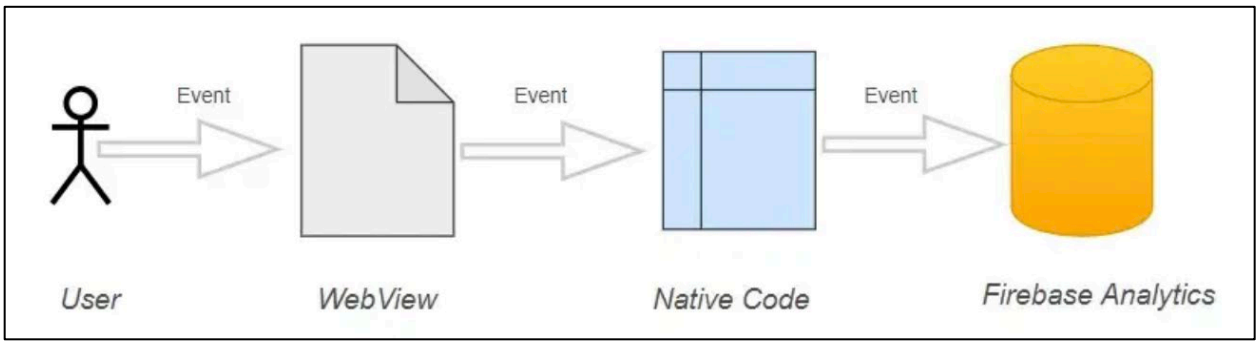
domain (e.g., YouTube, Reddit, Netflix). It is also helpful to distinguish between Google apps (which Google sometimes calls "owned-and-operated" or O&O, and "first-party" or 1P apps) and non-Google apps (which Google sometimes calls "third-party" or 3P apps), which may include apps that use Google services such as the Firebase SDK and Google Mobile Ads SDK. Well-known Google apps include YouTube, Gmail, Google Maps, Google Search, and Google Photos. Well-known non-Google apps include Reddit, Netflix, Amazon, Uber, New York Times, and many others.[64] On Android, many of these Google apps are pre-installed; others can be downloaded through the Google Play Store. On iOS, Google apps are available on the App Store. Users can also download non-Google apps from these app stores.

78. Apps can also incorporate web content directly into their apps, using webview technologies. As explained in documents Google produced in this litigation, "Webviews are a tool that iOS and Android app developers can use to get a browser-like experience in their custom applications. Webviews are not fully functioning web browsers but allow for browsing within an app" (GOOG-RDGZ-00041857 at -867). Another Google engineer explains that "webview is really just an implementation detail of the app. A developer may choose to have a mix of web + native views in their app, or swap out webview with a native view down the road, but ultimately from their business POV [point of view], it's 'an app'" (GOOG-RDGZ-00075692 at -692). Webviews are implemented in a way such that all browsing activities within a webview are conducted directly within the app (i.e., without taking the user to a standalone browser app). As

[64] A list of Google O&O apps available in Apple's App Store can be found at: https://apps.apple.com/us/developer/google-llc/id281956209?see-all=i-phonei-pad-apps and in Google Play Store at: https://play.google.com/store/apps/dev?id=5700313618786177705 (Last accessed February 15, 2023).

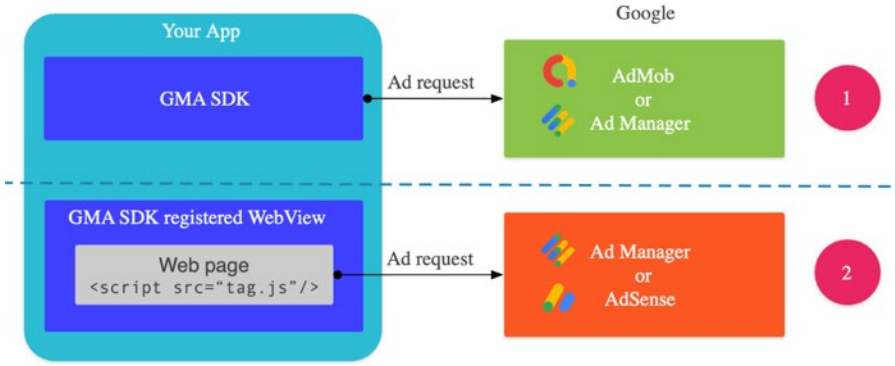
such, browsing activities within webviews are considered to be "app" activities, rather than "web" activities when associated with SDKs.[65]

79. Google tracks app activity that occurs within webviews, and it also serves advertisements within webviews. Google tracks activity in webviews using code called a "tag." A tag is a tracking beacon, meaning a program that collects data about a user's online activity and transmits that data to Google across the network. These tags are managed by Google Tag Manager (GTM), and to send this data to Google, the developer must have GA4F.[66] GA4F is implemented in a webview environment such that events in webview are sent to Google through Firebase.[67] Google explains to Firebase app developers that Analytics data collection within a webview environment "must be forwarded to native [app] code before they can be sent to Google Analytics … The first step in using Google Analytics in a WebView is to create JavaScript functions to forward events and user properties to native code."[68] This data flow is illustrated in the Figure below[69].



[65] "WebView solutions will treat webview traffic as app traffic when SDK signals are present" (GOOG-RDGZ-00149198 at -207).
[66] *Introduction to Mobile Tagging*, Google Tag Manager, https://developers.google.com/tag-platform/tag-manager/mobile (Last accessed February 15, 2023).
[67] Erhu Akpobaro, *Implementing Google Analytics for Firebase in Android Webview*, Google, https://firebase.google.com/codelabs/GA4F_Webview#0 (Last accessed February 15, 2023).
[68] *Use Analytics in a WebView*, Google, https://firebase.google.com/docs/analytics/webview?platform=android (Last accessed February 15, 2023). In its Answer to Plaintiff's Fourth Amended Complaint, Google admitted that "Android WebView is a pre-installed system component from Google that allows Android apps to display web content. Google admits that Google Analytics can be used with WebView" (Answer ¶ 68).
[69] Muffaddal Qutbuddin, *Firebase Analytics Event Tracking from WebView*, Medium, https://medium.com/swlh/send-events-from-webview-to-firebase-analytics-28d278f0bf4d (Last accessed February 15, 2023).

80. Within a webview environment, both Google Ad Manager and Google AdSense can serve ads as long as the app uses the Google Mobile Ads SDK as illustrated in the Figure below.[70] Google instructs app developers that if they want to use WebView to display web content that includes ads from Ad Manager or AdSense, they must use an API (application programming interface) to "register WebView objects with the Google Mobile Ads SDK."[71]



VII. OPINIONS

A. Google Has Collected WAA-off and sWAA-off Data Throughout the Class Period.

81. It is my opinion that throughout the class period, Google uniformly collected class members' WAA-off data and sWAA-off data, including a multitude of Google identifiers that Google uses to identify particular users. These Google identifiers include class members' GAIA ID and other identifiers that Google connects with GAIA ID on its servers.

82. Throughout this report, I will use the term "WAA-off data" to refer to data generated during a user's interaction with a non-Google mobile app while that user is signed into a Google account and her WAA toggle was set to "off" (or equivalently "paused" or "disabled").

[70] *Integrate the WebView API for Ads*, Google Ad Manager, https://developers.google.com/ad-manager/mobile-ads-sdk/android/webview (Last accessed February 15, 2023).
[71] *Integrate the WebView API for Ads*, Google Ad Manager, https://developers.google.com/ad-manager/mobile-ads-sdk/android/webview (Last accessed February 15, 2023).

83. I will use the term "sWAA-off data" to refer to data generated during a user's interaction with a non-Google mobile app while that user is signed into a Google account and her sWAA toggle was set to "off" (or equivalently "paused" or "disabled"). Note that sWAA-off data necessarily encompasses WAA-off data because sWAA cannot be turned on when WAA is turned off. However, a user can turn on WAA while turning off sWAA.

84. Google has collected WAA-off and sWAA-off data by way of Google Analytics for Firebase, app advertising products (i.e., AdMob and Ad Manager), and Firebase Cloud Messaging.

1. Google Analytics for Firebase

85. Irrespective of whether WAA or sWAA is set to on or off, Google has collected user data through Google Analytics for Firebase throughout the class period and across class members. Notwithstanding its public representations, Google admitted in this litigation that "WAA has never controlled whether Google Analytics for Firebase collects and sends user activity data from third party apps to Google servers" (Google's Supp. Resp. to Interrog. No. 4). WAA "functions independently from Google Analytics for Firebase," and therefore "turning off Web & App Activity does not prevent" Google from collecting data by way of Google Analytics for Firebase (Google's Resp. to RFA No. 1). Google processes user data "regardless of whether [they] have WAA on or off" (Google's Resp. to RFA No. 20).

86. My opinion is further supported by David Monsees[72] and Steve Ganem's deposition testimony that Google checks the user's WAA and sWAA status on its own servers, rather than the user's device.[73] That means that Google must collect and save data regardless of a user's WAA

[72] Mr. Monsees has been a Google employee since 2009 and is currently the product manager for Footprints (Monsees Tr. 18:21-22, 23:25-24:1).

[73] When questioned why Google Analytics would not check a local cache setting, like App Indexing, before uploading to Google servers, Mr. Monsees responded that "different services like Google Analytics might have other bases to process that data." Mr. Monsees further stated that he was not aware of any document that could explain "the logic behind the differences as to why some products with sWAA controls would check locally versus

and sWAA settings. Only after Google collects and saves app activity data does Google check the user's WAA and sWAA settings (Monsees Tr. 96:1-13), and even then Google saves WAA-off and sWAA-off data.[74] Google could have designed GA4F and the GMA SDK to check the user's WAA and sWAA settings on the device. Google's App Indexing product, for example, checks the user's device for the sWAA setting and does not send data to Google's servers if sWAA is off (Monsees Tr. 215:13-18, 303:4-10). Google chose not to design GA4F and the GMA SDK this way.

87. In the rest of this subsection, I explain the types of data and identifiers collected by Google Analytics for Firebase. As I discussed, WAA and sWAA settings have no impact on the types of data collected by Google app analytics products, including because a user's WAA and sWAA settings are not checked until data reaches Google servers. Even then, Google systematically saves and uses WAA-off and sWAA-off data for its own benefit. The data that Google collects and saves is essentially unaffected by the user's WAA and sWAA settings, except when sWAA is off, Google saves data only with persistent Google identifiers other than GAIA. In effect, the controls are a placebo. The user is given the choice whether they want to see some of the data Google collects and saves, or if the user would prefer to remain blissfully ignorant that Google is spying on their most private moments as they interact with their mobile devices.

88. Google Analytics for Firebase (GA4F) is a key component of Firebase and is included with the Firebase SDK implementation (GOOG-RDGZ-00187017 at -018). Documents that Google produced in this litigation confirm that GA4F provides "[c]omprehensive event-centric in-App

not check locally before uploading the data to Google servers," and that these decisions were "per service basis" (Monsees Tr. 216:24-218:1); *see also* Ganem Tr. 113:10-11.

[74] [redacted] (Monsees Tr. 310:8-20).

'behavioral' analytics" and an "[a]cross-network attribution tool" (GOOG-RDGZ-00187017 at -018).

89. Among other things, GA4F collects data about events, parameters, and user properties. Events are activities that users perform on an app, such as opening the app for the first time (a "first open"), loading a new page (a "screen view"), selecting content on a page ("select_content"), or making an in-app purchase (Answer ¶ 51). Google collects additional information about these events, and each piece of additional information is a "parameter." For example, when a user makes an in-app purchase, GA4F also collects an identifier for the product, as well as its price, currency, and quantity.[75] When a user loads a new page, GA4F also collects information about the identity of the page (page_title), the length of time the user spends on that page (engagement_time_msec), as well as information about the last page the user was on.[76] GA4F also collects "user properties," which are data about users themselves, as opposed to their activity (GOOG-RDGZ-00187017 at -018). User properties include age, gender, interests, operating system, location, language, and potentially even "favorite food."[77] While Google describes the collected events, parameters, and user properties to developers in online developer support pages, nowhere does Google disclose that it collects this data even if the user's WAA or sWAA setting is turned off.

90. Through GA4F, Google collects information about a "core set" of events, automatically and "[o]ut-of-the box" (GOOG-RDGZ-00187017 at -018). These events include "installs ('first opens')", "in-app purchases," operating system updates ("os_update"), the start of a session of app activity ("session_start"), and user engagement with the app ("user_engagement") (GOOG-

[75] *[GA4] Automatically Collected Events*, Google Analytics Help, https://support.google.com/analytics/answer/9234069?hl=en (Last accessed March 13, 2023).
[76] *[GA4] Automatically Collected Events*, Google Analytics Help, https://support.google.com/analytics/answer/9234069?hl=en (Last accessed March 13, 2023).
[77] *[GA4] User Properties*, Google Analytics Help, https://support.google.com/analytics/answer/9355671?hl=en (Last accessed March 13, 2023).

RDGZ-00187017 at -018; GOOG-RDGZ-00195309 at -490). GA4F includes "10+ automatically captured events" (GOOG-RDGZ-00187017 at -018). Indeed, Google acknowledges that "there are at least 26 events that can be collected through GA for Firebase automatically" (Answer ¶ 52).

91. Through GA4F, Google also collects a set of parameters automatically.[78] Each automatically collected event has a set of automatically collected parameters. These include, for example, "firebase_screen", "firebase_screen_class", "firebase_screen_id", "firebase_previous_screen", "firebase_previous_class", "firebase_previous_id", and "engagement_time_msec" for the "screen_view" event. Other events automatically collect parameters such as title of the page ("page_title"), data associated with the URL of the page ("page_location"), screen information (including "screen_resolution"), and session information.[79] Through GA4F, Google collects the mobile equivalents of a webpage URL and "referrer,"[80] which tells Google exactly which screen the user is viewing in the application. Google also uses GA4F to automatically collect other parameters only for specific events. For example, GA4F automatically collects price and value information associated with in-app purchases, but it does not collect this information when the user simply opens the app.[81] Through GA4F, Google "track[s] metrics such as user engagement or user behavior per screen."[82]

---

[78] *[GA4] Automatically Collected Events*, Google Analytics Help, https://support.google.com/analytics/answer/9234069?hl=en (Last accessed March 13, 2023).
[79] *[GA4] Automatically Collected Events*, Google Analytics Help, https://support.google.com/analytics/answer/9234069?hl=en (Last accessed March 13, 2023); Answer ¶ 54-56; Google's Resp. to Interrog. No. 1.
[80] In the 1990s computer scientist Phillip Hallam-Baker mis-spelled "referrer" as "referer" in a HTTP standards document, RFC 1945, and it stuck. *See HTTP Referer*, Wikipedia, https://en.wikipedia.org/wiki/HTTP_referer (Last accessed March 17, 2023).
[81] *[GA4] Automatically Collected Events*, Google Analytics Help, https://support.google.com/analytics/answer/9234069?hl=en (Last accessed March 13, 2023).
[82] *Measure Screenviews*, Gooogle, https://firebase.google.com/docs/analytics/screenviews#automatically_track_screens (Last accessed February 15, 2023).

92. Many of the events that Google automatically logs with GA4F, such as first opens and in-app purchases, are common conversion events. Conversion events are user activities that are considered important, and that developers and advertisers often seek to optimize. As explained by Belinda Langner, Google's 30(b)(6) designee and Product Manager for App Campaigns, "in the context of advertising" a conversion occurs when "a specific ad led to a specific action within the app," such as a "first open or [an] in-app purchase" (Langner Tr. 133:13-18; *see also* Ma Tr. 213:8-11).[83] Through GA4F, Google collects data that Google uses to track conversions driven by advertisers that place their ads with Google, and that Google serves through platforms like AdMob (Ganem Tr. 28:21-25).

93. Through GA4F, Google also automatically collects certain user properties. These include age, gender, interests, app version, operating system version, language, first launch time, and device model, and many other pieces of information (GOOG-RDGZ-00187017 at -018; Google's Resp. to Interrog. No. 1).

[83] *See also* Langner Tr. 133:20-23 ("advertisers are able to define their -- the app events that they care about, and so certainly, advertisers define other types of events").

94. Some of the events and user properties that GA4F automatically collects are shown in the figure below, which is excerpted from a 2016 document (GOOG-RDGZ-00195309 at -490).[84]

95. Altogether, GA4F collects a surprising amount of data. According to documents Google produced in this case, GA4F can collect "up to *500* different event types," with "*25* parameters per event," while simultaneously collecting detailed data about the user "such as Age, Gender, Interests, App Version, and OS Version" and potentially dozens more pieces of information (GOOG-RDGZ-00187017 at -018). GA4F can also "create up to 50 audiences by combining event data and user properties," and track specific events designated as "conversions" (GOOG-RDGZ-00187017 at -018).

96. GA4F can be integrated with many other Google products, including Google AdMob, Google Play[85], Google Ads, Firebase Cloud Messaging, and Firebase Crashlytics (GOOG-RDGZ-00050615 at -615). "Google Analytics has integrations with other products which may collect their

[84] *See also* GOOG-RDGZ-00028218 at -219 and -220. The document lists some of the automatically captured events by GA4F, including first_open, in_app_purchase, error, user_engagement, session_start, app_update, os_update, app_clear_data, notification_foreground, notification_receive, notification_open, notification_dismiss. Some of the automatic user properties collected include app version, device model, interests, gender, age, OS version, app store, first open date and new/established. In addition to automatically logged events, GA4F can also log recommended events and custom events specified by app developers. *Log Events*, Google, https://firebase.google.com/docs/analytics/events?platform=android (Last accessed February 15, 2023).

[85] In Google's Answer to Plaintiff's Fourth Amended Complaint, "Google admits that Firebase SDK provides support for Google Play and that Google Play is a platform through which app developers can distribute their app to users and process payments" (Answer ¶ 41).

own data separately and log them to different log sources and where there are integrations between these products, it may be that certain data from one product then later flows into another product, which is the nature of integrations" (Ganem Tr. 53:7-14).

97. As I discussed above, Google uses GA4F to collect and save data relating to user activity within apps, either natively or within Webview. The events, parameters, and user properties that Google uses GA4F to collect and save in Webview are also extensive.

98. A Google help page summarizes the events that Google automatically collects and saves using GA4, which, as I explained previously, is the current generation of Google Analytics for apps and the web, built atop the GA4F architecture. These events are identified in the table below, and events denoted "web" are applicable in Webview[86]:

Event	**Automatically triggered…**
ad_click	when a user clicks an ad
ad_exposure	when at least one ad served by the Mobile Ads SDK is on screen
ad_impression	when a user sees an ad impression
ad_query	when an ad request is made by the Mobile Ads SDK
ad_reward	when a reward is granted by a rewarded ad served by the Mobile Ads SDK
adunit_exposure	when an ad unit served by the Mobile Ads SDK is on screen
app_clear_data	when the user resets/clears the app data, removing all settings and sign-in data Android only
app_exception	when the app crashes or throws an exception
app_remove	when an application package is removed (uninstalled) from an Android device Android only
app_store_refund	when an in-app purchase is refunded by Google Play Android only
app_store_subscription_cancel	when a paid subscription is cancelled in Google Play Android only
app_store_subscription_convert	when a free-trial subscription is converted to a paid subscription
app_store_subscription_renew	when a paid subscription is renewed
app_update	when the app is updated to a new version and launched again
click (web)	each time a user clicks a link that leads away from the current domain
dynamic_link_app_open	when the app is updated to a new version and is opened via a dynamic link Android only
dynamic_link_app_update	when the app is updated to a new version and is opened via a dynamic link Android only

[86] *[GA4] Automatically Collected Events*, Firebase Help, https://support.google.com/firebase/answer/9234069 (Last accessed February 15, 2023).

Event	Automatically triggered…
dynamic_link_first_open	when a user opens the app for the first time via a dynamic link
error	logged in place of an event that can't be logged because it is invalid in some way
file_download (web)	when a user clicks a link leading to a file
firebase_campaign	when the app is launched with campaign parameters
firebase_in_app_message_action	when a user takes action on a Firebase In-App Message
firebase_in_app_message_dismiss	when a user dismisses a Firebase In-App Message
firebase_in_app_message_impression	when a user sees a Firebase In-App Message
first_open	the first time a user launches an app after installing or re-installing it
first_visit	the first time a user visits a website or launches an Android instant app with Analytics enabled
form_start (web)	the first time a user interacts with a form in a session
form_submit (web)	when the user submits a form
in_app_purchase	when a user completes an in-app purchase, including an initial subscription, that is processed by the Apple App Store or Google Play Store
notification_dismiss	when a user dismisses a notification sent by Firebase Cloud Messaging (FCM) Android only
notification_foreground	when a notification sent by FCM is received while the app is in the foreground
notification_open	when a user opens a notification sent by FCM
notification_receive	when a notification sent by FCM is received by a device when the app is in the background Android only
notification_send	when a notification is sent by FCM Android only
os_update	when the device operating system is updated to a new version.
page_view (web)	each time the page loads or the browser history state is changed by the active site
screen_view	when a screen transition occurs
scroll (web)	the first time a user reaches the bottom of each page (i.e., when a 90% vertical depth becomes visible)
session_start	when a user engages the app or website
user_engagement	when the app is in the foreground or webpage is in focus for at least one second.
video_complete (web)	when the video ends
video_progress (web)	when the video progresses past 10%, 25%, 50%, and 75% duration time
video_start (web)	when the video starts playing
view_search_results (web)	each time a user performs a site search, indicated by the presence of a URL query parameter

99. With GA4F, Google also collects and saves user dimensions relating to users in native app and Webview, including sensitive user information such as age, gender, location, interests,

location, and device information. Automatically collected user dimensions are summarized in the table below, also based on a Google help page[87]:

User dimension	Description
Age	The age of the user by bracket: 18-24, 25-34, 35-44, 45-54, 55-64, and 65+.
App store	The store from which the app was downloaded and installed.
App version	The versionName (Android) or the Bundle version (iOS).
Browser (web)	The browser from which user activity originated.
City	The city from which user activity originated.
Continent	The continent from which user activity originated.
Country	The country from which user activity originated.
Device brand	The brand name of the mobile device (such as Motorola, LG, or Samsung).
Device category	The category of the mobile device (such as mobile or tablet).
Device model	The mobile device model name (such as iPhone 5s or SM-J500M).
Gender	The gender of the user (male or female).
Interests	The interests of the user (such as Arts & Entertainment, Games, Sports).
Language	The language setting of the device OS (such as en-us or pt-br).
New/Established	New: First opened the app within the last 7 days. Established: First opened the app more than 7 days ago.
Operating system	The operating system used by visitors to your website or mobile app.
OS version	The operating system version used by visitors to your website or mobile app (such as 9.3.2 or 5.1.1).
Platform	The platform on which your website or mobile app ran (such as web, iOS, or Android).
Region	The geographic region from which user activity originated.
Subcontinent	The subcontinent from which user activity originated.

a. Identifiers Used and Issued by Google

100. Google uses GA4F to collect and save a multitude of identifiers for specific events, apps, devices, and users, in addition to events and user properties.

101. One of the identifiers that Google collects and saves via GA4F is the GAIA ID, which is unique to the user's Google account. Google collects the user's GAIA ID regardless of their WAA or sWAA status; the user's WAA or sWAA status affects the locations and time for which data is saved alongside the GAIA ID. When the user has turned off WAA or sWAA, their data may still

[87] *[GA4] Predefined User Dimensions*, Firebase Help, https://support.google.com/firebase/answer/9268042 (Last accessed February 15, 2023).

be stored with an encrypted version of their GAIA ID. One encrypted form of the GAIA ID is called DSID, which Google can use to do conversion tracking and check the user's consent status (Google's 4th Supp. Resp. to Interrog. No. 1, § 1; GOOG-RDGZ-00071768, "Measurement Bundle Proto" tab, Row 36; Ganem Tr. 64:3-9, 67:18-20). Google logs and uses DSID even when the user has WAA or sWAA off (Langner Decl. (March 2, 2023)).[88]

102. With GA4F, Google also collects and saves identifiers that are unique to a device, including Identifier for Advertiser (IDFA) for iOS devices and Advertising ID (ADID) for Android devices (sometimes collectively called "device IDs") (Google's 4th Supp. Resp. to Interrog. No. 1, § 2; GOOG-RDGZ-00147439 at -450). These are "random device identifier[s]" assigned to the device by Apple and Android, respectively (GOOG-RDGZ-00056142 at -157). These identifiers are used for, among other things, tracking and measuring conversions (Google 4th Supp. Resp. to Interrog. No. 1, § 2; Langner Tr. 49:16-21, 185:13-17). IDFA and ADID are the same for all apps on a single device, and so they can be used track a user's activities (including analytics and ads data) across all apps on the device (GOOG-RDGZ-00147439 at -450). The user's WAA and sWAA settings do not impact Google's collection of IDFA and ADID using GA4F.

103. Another such identifier is the Identifier for Vendors (IDFV) from iOS users. As Steve Ganem, Google's 30(b)(6) designee and Director of Product Management for Google Analytics, testified at his deposition, IDFV is an identifier that is unique per device, per app publisher (Ganem Tr. 232:13-21). It is assigned by iOS the first time a user downloads an app from a distinct app publisher on their device; when the user downloads a second app from the same publisher, then the same IDFV will be used (Ganem Tr. 237:20-238:9). Users cannot reset their IDFV (GOOG-

[88] Google represents that developers can opt out of DSID collection by disabling a setting called Google Signals, which was an integration between Google Analytics and Google signed-in data (Google 4th Supp. Resp. to Interrog. No. 1, § 1; Stone Tr. 35:3-6; GOOG-RDGZ-00176250).

RDGZ-00071867 at -867). Through GA4F, Google collects IDFV, at least when IDFA is unavailable (for example, if the user enables the Limit Ad Tracking (LAT) or App Tracking Transparency (ATT) settings) (Ganem Tr. 232:13-21).[89] Google uses GA4F to collect IDFV regardless of the user's WAA and sWAA settings.

104. On Android devices, when ADID is not available, Google may collect an Android ID called SSAID (if enabled by the app developer[90]). "This alternative Android identifier cannot be reset," and so Google engineers fairly asked: "The concern is privacy, if a user opt[s] to not share AdID why would we default to collect a[n] even less private ID" (GOOG-RDGZ-00100645). ADID might be unavailable in the unusual circumstance that the user exercised the option (first provided in 2021) to delete their ADID.[91]

105. Google also uses GA4F to collect and save the user's IP address, including for geolocation lookup (Google's 4th Resp. to Interrog. No. 1, § 2).

106. Google also uses GA4F to collect and save other identifiers that are unique to the device, such as app instance id, sometimes called a Client ID (Google's 4th Resp. to Interrog. No. 1, § 1; GOOG-RDGZ-00207704). As explained by Google's 30(b)(6) designee and Group Product Manager for Google Analytics, app instance id refers to a GA4F-assigned identifier that is a "unique installation of an app on a device" (Ganem Tr. 92:20-23, 99:7-9; Google's 4th Supp. Resp.

[89] The developer has the option to opt-out of IDFV (GOOG-RDGZ-00052600 at -600). In April 2021, Apple replaced LAT with a new privacy framework called App Tracking Transparency (ATT) as a part of the iOS 14.5 rollout. *Upcoming AppTrackingTransparency Requirements*, Apple Developer, https://developer.apple.com/news/?id=ecvrtzt2 (Last accessed March 16, 2023).

[90] "On Android Firebase Analytics SDK will collect and report the Android ID (a.k.a. SSAID) on devices that do not have Google Play Services installed" (GOOG-RDGZ-00180316 at -325) and "If the developers implements the opt-out for IDFV/SSAID collection, then we will not collect IDFV/SSAID, specifically" (GOOG-RDGZ-00052600 at -600).

[91] GOOG-RDGZ-00052600 at -600; Bennett Cyphers, *How to Disable Ad ID Tracking on iOS and Android, and Why You Should Do It Now*, EFF, https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now (Last accessed February 15, 2023); ADID opt out rate appears to be very low (3-5%) (GOOG-RDGZ-00208099 at -104).

to Interrog. No. 1, § 1). Each person's Uber application, for example, has a different app instance id. An app instance id is distinct from an app id, which is unique to the app itself, across devices (GOOG-RDGZ-00059808 at -810). Google also uses GA4F to collect and save app id (Ganem Tr. 99:7-9). The app instance id can be reset, primarily when the user re-installs an app, makes certain updates to an app, or resets their advertising identifier (Google's 4th Supp. Resp. to Interrog. No. 1, § 1 on Data Logging).

107. Google also uses GA4F to collect and save Firebase Instance ID (FID), also known as an IID, which is also a unique identifier for an instance of an app installed on a device (GOOG-RDGZ-00207704 at -704; Google's 4th Supp. Resp. to Interrog. No. 1, § 2 on Data Logging Technical Details). Whereas app instance id is a GA4F ID, IID is a Firebase ID. Google's internal document explains that "through its association with Android ID and GServices AID, IID (which is unique per app-device combination) can be mapped to GAIA on Google's backend" (GOOG-RDGZ-00207704 at -705).

108. Google also uses GA4F to collect and save identifiers that it assigns to a specific event, performed by a specific user. For example, an "Ad Event ID" (or aeid) is assigned when a user has an interaction with an ad (e.g., an impression, a click); when a different user has the same interaction with the same ad, or when the same user has the same interaction with the same ad at a different time, a different Ad Event ID will be assigned (Google's 4th Supp. Resp. to Interrog. No. 1, § 1). Google explains that it uses GA4F to collect and save Ad Event ID, "in order to enable integration between GA for Firebase and AdMob" (Google's 4th Supp. Resp. to Interrog. No. 1, § 1).

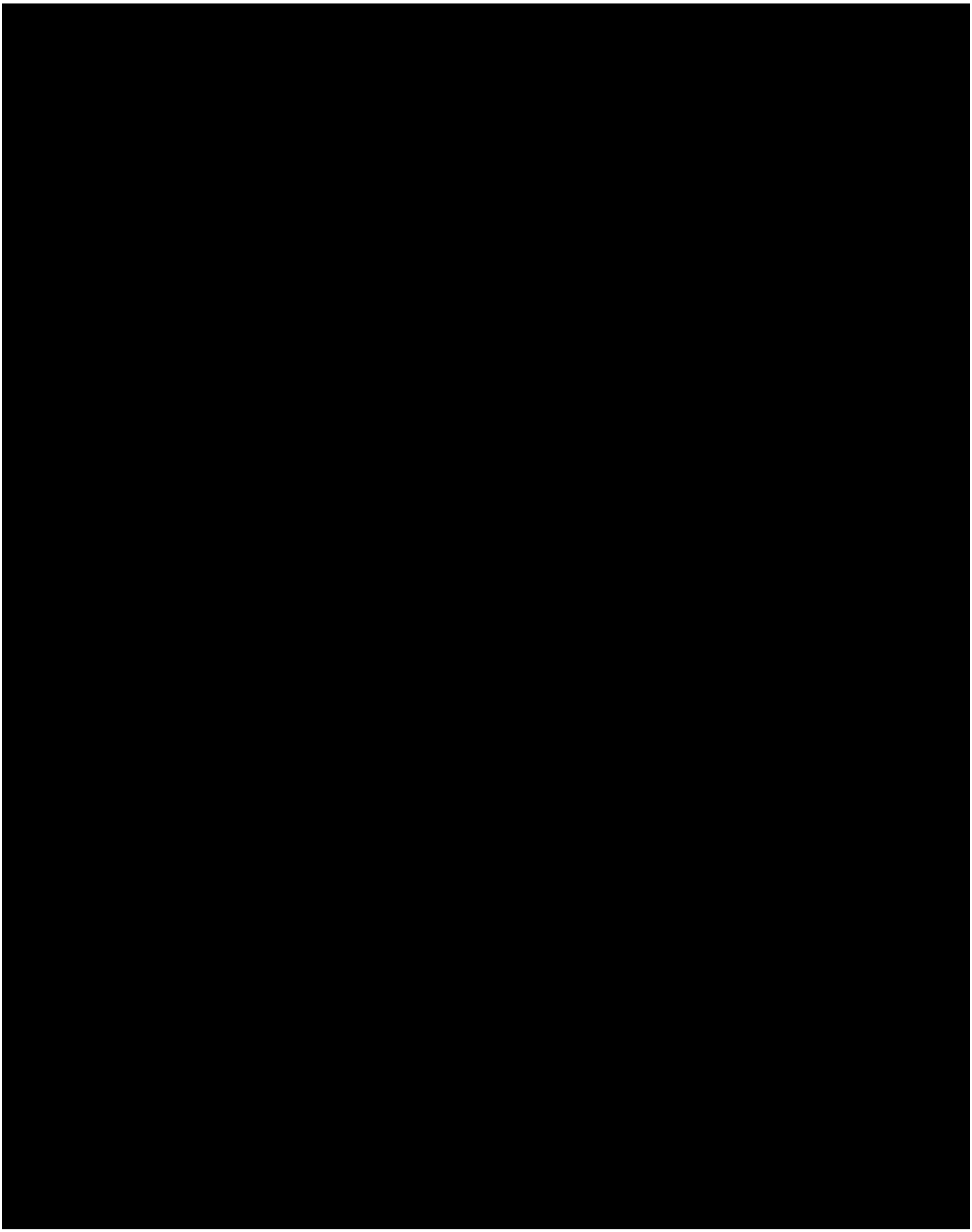
109. Google also uses GA4F to collect and save User ID, which app developers may assign to identify a specific user signed into their app, just as GAIA ID uniquely identifies a Google account

holder.[92] User ID is a "persistent identifier for a single user across one or more sessions initiated from one or more devices," (GOOG-RDGZ-00056142 at -157) which can "tie user activities across platform/devices" (GOOG-RDGZ-00196620 at -656). Although an app developer theoretically could change the User ID for their users, based on my experience with Google Analytics and my understanding that app developers use User IDs to identify users, I believe it is unlikely that app developers change the User IDs for their users.

110. I have described only a small fraction of the identifiers that Google uses GA4F to collect and save. Other documents reveal dozens upon dozens of additional identifiers. For example, in a spreadsheet titled "Unique ID Analysis," Google lists [redacted] identifiers (GOOG-RDGZ-00181081). That list is reproduced below:

[redacted]

[92] *[GA4] Measure Activity Across Platforms with User-ID*, Google Analytics Help, https://support.google.com/analytics/answer/9213390 (Last accessed February 15, 2023); GOOG-RDGZ-00082288 at -289 ("Do we have any viable alternatives outside of using the User ID in this manner?...There is no alternative or better identifier for analysis or targeting than the customers self-identified login which represents a 1:1 relationship between our client and their customers…We could alternatively use Google Signals ([redacted]) which also deduplicates users based on logged in data – and for us all would be logged in on [redacted], so it's pretty much the same in that respect").



111. Other identifiers are listed in a document called "Many IDs of Android and iOS" (GOOG-RDGZ-00208197).

112. Google links many of these identifiers together. Through internal mechanisms such as [redacted] for example, Google links IDFA and ADID to other Google identifiers, such as Zwieback (which is associated with Google Search) and Biscotti (which is associated with display ads), which, together with GAIA, enable Google's ads integrations (GOOG-RDGZ-00176250 at -250; GOOG-RDGZ-00056108 at -114, -115). Google also maintains "a mapping of Firebase Installation Ids (FID…) to their corresponding Custom user ids" (GOOG-RDGZ-00078400 at -404). I will discuss ID mappings and linkages in more detail in Section VII.G.

113. Google internally distinguishes between identifiers that are "owned" by third-party apps and identifiers that are "owned" by Google. For example, Google considers app instance id[93] (which is issued by GA4F) and User ID to be "owned" by third-party apps, while ADID and IDFA are not (GOOG-RDGZ-00056142 at -157). According to documents that Google produced in this

[93] Although Google considers app instance id to be "customer-owned", Google acknowledges that this ID is generated by GA4F (GOOG-RDGZ-00056142 at -157).

case, Google uses identifiers even if they are "owned" by third-party apps. One document explains that "customer-owned" IDs "are leveraged for analytics and measurement purposes" and the IDs that are not customer-owned "are typically used for audience personalization and bidding" (GOOG-RDGZ-00056142 at -157).

b. Analytics Hit Bundles

114. GA4F data is collected in packets or bundles, sometimes called "HitBundles" (Google's 4th Supp. Resp. to Interrog. No. 1, § 3). Regardless of the user's WAA and sWAA settings, HitBundles contain ([redacted]) (b) [redacted]), and (c) user properties (Google's 4th Supp. Resp. to Interrog. No. 1, § 3). HitBundles may also contain ADID (Ganem Tr. 225:18-20). Internal Google documentation depicts the construction of these HitBundles:

[redacted]

115. As I will explain in Section VII.B.2, event data from users who have turned off WAA or sWAA is sent to Google in the same packets as identifying information, including but not limited to name, email address, and device identifiers.

116. GA4F also sends HitBundles to Google's servers periodically. This means that a single HitBundle may include data from events that occurred days, weeks, or months apart. When Google performs its consent check, however, it checks user settings only at the time Google's servers receive the HitBundle; it does not check the user's consent status at the time of each event (Google's 4th Supp. Resp. to Interrog. No. 1, § 3 and 4). If a user turns on their WAA or sWAA settings between the time of an event and the time the HitBundle is processed by Google's servers, that data may be collected and saved alongside the user's GAIA ID.

117. For Android users, a single HitBundle may also contain data from multiple apps. If an Android app has Google Play Services enabled, then Google uses GA4F to collect data in a central, cross-app file [redacted], which is periodically uploaded to Google's servers (Google's 4th Supp. Resp. to Interrog. No. 1, § 3). This file—and resulting HitBundles—contain a view of the user's activity across apps, regardless of their WAA and sWAA settings. On iOS devices, Google does not have access to a central file where it can use GA4F to collect and save data. Instead, GA4F periodically transmits data from each app to Google's servers individually (Google's 4th Supp. Resp. to Interrog. No. 1, § 3).

2. Google's App Advertising Products

118. Google's app advertising products include the Google Mobile Ads (GMA) SDK (which supports Google Ad Manager and Google AdMob, including AdMob+, which incorporates analytics functionality from GA4F). According to Google's internal documentation, the sWAA setting relates to Display Ads, which includes ads shown in non-Google apps (GOOG-RDGZ-00042318 at -326).

119. Based on documents that Google produced in this case, the testimony of Google's employees and Google itself (including through interrogatory responses and Google's 30(b)(6) designees), and my testing of Google's collection and saving of data related to apps that use these Google advertising products, it is my opinion that Google uses these app advertising products to collect and save app activity data even if the user has turned off their WAA or sWAA settings.

120. As with GA4F, Google checks the user's consent status on its servers, after collecting and saving the data. David Monsees, Google's 30(b)(6) designee and Product Manager in the Footprints team, explained that Google first collects and saves an ad request without knowing "if WAA was on or not" (Monsees Tr. 96:1-13). Google checks the user's WAA and sWAA status only after the ad request "hits the Google server" (Monsees Tr. 96:1-13). Google's internal documentation describing the "[l]ife of an ad request" confirms Mr. Monsees's understanding (GOOG-RDGZ-00028472 at -474). According to that document, a Google server called [redacted] "[h]andles all policy enforcement details" (i.e., works with other servers to check WAA and sWAA status) (GOOG-RDGZ-00028472 at -474). The ad request itself does not contain the user's WAA or sWAA setting states; Google must use an identifier to look up the user's status (Monsees Tr. 96:1-13, 101:24-102:4).

121. Like GA4F, Google uses its app advertising products to collect a wide variety of data, including events, parameters, and user properties.

122. The Google Mobile Ads SDK, for example, automatically sends data relating to several types of ad events. These include ad requests, in which an app that uses AdMob, Ad Manager, or AdSense asks Google for an ad to display; ad impressions, in which an ad is shown in an app; ad views, in which the user views an ad displayed in the app; and ad clicks, in which the user clicks on an ad. In Google's Answer, it admits that the Google Mobile Ads SDK collects "app-

interaction[]" data "such as ad clicks and ad impressions" (Answer ¶ 66). The collection and saving of an ad request are the first steps in Google's process of delivering an ad—a large part of Google's business model. If Google did not collect and save ad requests, it could not serve ads. And without data regarding both ad requests and the ads that Google served, Google would lack the records it needs to charge advertisers for its services.[94] Google also uses this ads data to track conversions; if it lacked data regarding a user's interaction with an ad, it would be unable to determine whether that interaction is related to any later behavior.[95]

123. As with GA4F, Google uses the Google Mobile Ads SDK to collect and save this event data with substantial amounts of additional information. This information includes, but is not limited to, IP address, timestamp, device identifiers (including ADID and IDFA), information about the device (including location), and information about the ad content served (GOOG-RDGZ-00164383 at -387; GOOG-RDGZ-00206388 at -399).

124. The GMA SDK also sends other identifiers, such as the GAIA ID. As explained by internal Google documentation, "For Android devices…the AdMob SDK obtains the GAIA-ID for the default account signed into the device and creates a [redacted] which is passed with every AdMob ad request. For convenience of processing, the Gaia ID is passed in the same format as the DSID cookie" (GOOG-RDGZ-00147439 at -452). The GMA SDK also sends an AdMob app ID (admob_app_id), which identifies an AdMob app account (GOOG-RDGZ-00058520 at -520).

[94] *E.g. Click Measurement Guidelines* at 16, Interactive Advertising Bureau, https://mediaratingcouncil.org/standards-and-guidelines (Last accessed March 17, 2023) (discussing "auditing guidelines," which include "counting methods"); *Mobile Application Advertising Measurement Guidelines* at 20, Interactive Advertising Bureau, https://mediaratingcouncil.org/sites/default/files/Standards/Mobile%20InApp%20Measurement%20Guidelines%20%28MMTF%20Final%20v1.1%29.pdf (Last accessed March 19, 2023) (same).

[95] *E.g.*, GOOG-RDGZ-00195736 at -37 (describing [redacted] "conversion window[s]" for Google to connect the data).

Google Ad Manager 360 customers may also send an ID called [redacted] which uniquely identifies a user signed in on the app.[96]

125. The integration of AdMob with Firebase was discussed in Section VI.D. With the integration of AdMob and Firebase since 2016, the AdMob SDK obtained three IDs from GA4F (or Scion): gmp_app_id (a Firebase app account ID[97]), app_instance_id (which uniquely identifies an instance of an app on a device) and event_id (identifying a particular event[98]). These IDs are then sent along with ad events, including ad requests, ad impressions, active views and ad clicks. This is shown in the Figure below taken from GOOG-RDGZ-00057753 at -774. As explained by the figure, AdMob and Analytics data are joined in the Google backend through these three IDs. Because these IDs are present in both AdMob and Analytics logs and can be used to join other data in those logs, they are referred to as "join keys."

[96] *Targeting*, Google Ad Manager, https://developers.google.com/ad-manager/mobile-ads-sdk/android/targeting#publisher_provided_identifiers (Last accessed February 15, 2023).
[97] GOOG-RDGZ-00066207 at -210 (explains that the "gmp_app_id is Google Mobile Platform app id, used in firebase to identify an app" and "app_instance_id use to identify a device + app, differs for each app instance").
[98] Google's Fourth Supplemental Response to Interrogatory No. 1, Section 1 on Data Logging, further explained "GA for Firebase also logs aeid, or 'Ad Event ID,' which is a unique identifier for the specific ad interaction logged in order to enable integration between GA for Firebase and AdMob if the customer has linked their AdMob app to Google Analytics."

126. As Google has explained, the integration between GA4F and the Google Mobile Ads SDK allows for the collection and saving of app-usage and ads data, for further measurement and analysis (Google's Supp. Resp. to Interrog. No. 23). Google explains that "[b]ecause the GA for Firebase infrastructure supports the integration, the app-usage data available for measurement is the same data available for measurement through GA for Firebase and described in Google's Response to Interrogatory No. 1," which describes the data that Google collects and saves using GA4F.

127. AdMob+, which uses the Google Mobile Ads SDK, also collects and saves both ads data and analytics data. For apps that use AdMob+, Google joins ads and analytics data with "[redacted]d,"[99] and Google also uses either "[redacted]" (depending on whether the Firebase SDK is present), not both" (GOOG-RDGZ-00065831 at -833

[99] Steve Ganem testified that "AdMob+'s use of app measurement infrastructure" uses the "app instance ID as a pseudonymous identifier" (Ganem Tr. 108:9-11).

to -834). If the app uses the Firebase SDK, it uses [redacted]; if Firebase SDK is not present, Google uses [redacted] (GOOG-RDGZ-00065831 at -833 to -834).

128. Google also uses an identifier called a [redacted] in its advertising business. According to documents Google produced in this litigation, "[o]ne of the first steps performed by the display ads system is to map the IDFA/AdID to a [redacted] ([redacted] when it is important to differentiate from the Biscotti ID stored in browser cookies)" (GOOG-RDGZ-00206388 at -399).[100] I will discuss [redacted] in more detail in Section VII.G.

129. With the launch of AdMob+ in the summer of 2019 (GOOG-RDGZ-00031656), Google began to use the Google Mobile Ads SDK to automatically collect and save additional events,[101] including the following:

Event	**Automatically triggered…**
ad_click	when a user clicks an ad
ad_exposure	when at least one ad served by the Mobile Ads SDK is on screen
ad_impression	when a user sees an ad impression
ad_query	when an ad request is made by the Mobile Ads SDK
ad_reward	when a reward is granted by a rewarded ad served by the Mobile Ads SDK
adunit_exposure	when an ad unit served by the Mobile Ads SDK is on screen
app_clear_data	when the user resets/clears the app data, removing all settings and sign-in data Android only
app_exception	when the app crashes or throws an exception
app_remove	when an application package is removed or "uninstalled" from an Android device Android only
app_update	when the app is updated to a new version and launched again
first_open	the first time a user launches an app after installing or re-installing it
in_app_purchase	when a user completes an in-app purchase, including an initial subscription, that is processed by the App Store on iTunes or by Google Play
os_update	when the device operating system is updated to a new version.
screen_view	when a screen transition occurs
session_start	when a user engages the app for more than the minimum session duration after a period of inactivity that exceeds the session timeout duration
user_engagement	periodically, while the app is in the foreground.

[100] Google also refers to the Google Mobile Ads SDK as the AdMob SDK (Weng Tr. 59:9-12).
[101] *Automatically Collected Events*, Google AdMob Help, https://support.google.com/admob/answer/9755157 (Last accessed February 15, 2023).

Google also uses the Google Mobile Ads SDK to automatically collect and save user properties,[102] including:

User dimension	Description
Age	Identifies users by six categories: 18-24, 25-34, 35-44, 45-54, 55-64, and 65+.
App Store	The store from which the app was downloaded and installed.
App -Version	The versionName (Android) or the Bundle version (iOS).
Country	The country the user resides in.
Device Brand	The brand name of the mobile device (e.g., Motorola, LG, or Samsung).
Device Category	The category of the mobile device (e.g., mobile or tablet).
Device Model	The mobile device model name (e.g., iPhone 5s or SM-J500M).
First Open Time	The time (in milliseconds, UTC) at which the user first opened the app, rounded up to the next hour.
Gender	Identifies users as either male or female.
Interests	Lists the interests of the user (e.g., "Arts & Entertainment, Games, Sports").
Language	The language setting of the device OS (e.g., en-us or pt-br).
New/Established	New: First opened the app within the last 7 days. Established: First opened the app more than 7 days ago.
OS Version	The version of the device OS (e.g., 9.3.2 or 5.1.1).

130. By way of example, below I show an AdMob ad request sent from an Android device to Google. The ad request contains both DSID and Biscotti (here, listed as "IDE") cookies, user-agent (describing the type and version of device and operating system), the app sending the request (Picsart), and Ad Event ID (aeid), among other information. What is not shown below is the user's public IP address, which Google necessarily collects because the IP address is part of every IP packet.

```
GET /mads/gma?
[redacted] &
android_app_volume=1 &
disable_ml=false &
adid_p=1 &
format=320x50_mb &
omid_v=a.1.3.3-google_20200416 &
is_nonagon=true &
```

[102] *Automatically Collected User Properties*, Google AdMob Help, https://support.google.com/admob/answer/9755590 (Last accessed February 15, 2023).

android_app_muted=false &
am=0 &
dv=221310604 &
gl=US &
hl=en &
js=afma-sdk-a-v221310999.214106000.1 &
lv=0 &
ms=CrADCqsDmsA_ATEaOwGlVES8qPtvaRvJpA7BLpQBpFIYIzevDeocfifRCk1OaMYd9BdE8odD1w197BiXdNv-IsIgZpVb9zKhEuYCKC1DBQYs7zpRLTx_JDQBcjUnBkdcCj2etiUBaHkNgrkSqOe0OrSfADfRsWVuZjBN8zqjA0gyjBpvUgtXFO69xQjGBGtou6QGZAQPO5EcijKPqLTl_g2UtrHQn3IwRNCUdENT6OVYa0tTsNX5biufiGnKXIx2m2oTEGU4z8Bmbz3uxMo4hoSNijfN6jdhhAkCKTLHux2nyl6RRGPkkkT_6SXxa4Lk5JZM9winIPu5dupzn16rpL4En8J7-3UmoKmkIqvFRW9zNhPP3c6X30tBl3uhHKhPapRB3M2wWhFzvvHmm1nIRDfAtRS5dC0ft1bPu13IfqOdBSTTxQXW4jGGKtA1BWJbvubSbvK54yHsp6GKOW4bBdSyCwb34vssxNDPCCld5QGf3_uFqRHcPEnVhZpwJvpDrEaquXVQxyv9lXsWsxj7AV_2bDZuB0uh9d-SwGZ2mQrHWVYIUg5RJqQnhAHPY1iaMyAEEpUCCoACW4Z__D6ef8hCyNbAep53XiyOJReEzKo1G3r8IIZHhTQSNP5kSPJDNxnISZhCs8L692hWQPFHQOyoZpP6Lbu4Ew5Vm73Xn4Oe_SjKc6TiPUHdz3cHewIDD1YQb5DhcLQYjqlRBQbZDi4rdb6d2cax7xfM_yMdFsQ3BQwaeb8norQKpg8-hPv5pU9TVEnVFrluLQH_C8Qp4wrTKV5UjnjqdlctdUhvCIZSc-kIT2rt2Dowlkg4k5M2a61BUP2J_MrwifU5WJ51FA-dccJQVfz8fjmemQPKSIEzTRQWrB0SlBgUzpx4uGFdG1P5tRPxwCfxme1rxrHqhE_g9svQc-HYRIQ940i1i71pcLCUQmpQBFr2w &
mv=83061610.com.android.vending &
rm=2 &
sp=false &
coh=true &
riv=11 &
vnm=19.9.4 &
u_sd=3 &
request_id=1950993468 &
render_in_browser=false &
target_api=31 &
app_open_version=2 &
is_sidewinder=0 &
request_agent=applovin &
[redacted]
seq_num=14 &
is_gbid=false &
eid=318496669%2C318500618%2C318486317%2C318491267%2C318482078%2C318482960%2C318483611%2C318484497%2C318492496%2C318498028%2C318500128%2C318500151%2C318500344%2C318501236%2C318503634%2C318503836%2C318484910%2C318475418%2C318501444%2C318495468 &
tag_for_child_directed_treatment=0 &
_c_csdk_npa_o=false &

guci=0.0.0.0.0.0.0.0 &
sdk_apis=7%2C8 &
omid_p=Google%2Fafma-sdk-a-v221310999.214106000.1 &
cap=m &
u_w=360 &
u_h=723 &
msid=com.picsart.studio &
an=993819904.android.com.picsart.studio &
_package_name=com.picsart.studio &
u_audio=3 &
net=wi &
u_so=p &
adk=4015525142 &
preqs_in_session=18 &
support_transparent_background=true &
preqs=13 &
time_in_session=1139600 &
output=html &
region=mobile_app &
u_tz=-420 &
client=ca-app-pub-1876933753768597 &
slotname=1269794617 &
gsb=wi &
ogsb=wi &
apm_app_id=1%3A1076413845392%3Aandroid%3A889e98bb9f99c4e2 &
gmp_app_id=1%3A1076413845392%3Aandroid%3A889e98bb9f99c4e2 &
apm_app_type=1 &
lite=1 &
caps=inlineVideo_interactiveVideo_mraid1_mraid2_mraid3_sdkVideo_exo3_th_autoplay_medi
ation_scroll_av_av_transparentBackground_sdkAdmobApiForAds_di_aso_sfv_dinm_dim_nav_
navc_dinmo_ipdof_gls_xSeconds &
bisch=true &
blev=1 &
canm=false &
_mv=83061610.com.android.vending &
heap_free=5608784 &
heap_max=536870912 &
heap_total=202498720 &
wv_count=1 &
rdps=95800 &
blockAutoClicks=true &
trt=0 &
includeDoritos=true &
includeCookies=true &
session_idl=18 &
rdidl=36 &

idtypel=4 &
attokl=524 &
is_latl=-1 &
blob=ABPQqLE3SSp0vQUpyMDoEIXWPOtHF0x4bwGuetD058Qktc5MgvFc8fYRufGe7sEN
xiiCzGw-
96SMtadb44ktUiwk3chwnCDnkUUhv3NVj7hWr3HilUoq0lSThiaaRFT705RnVJi9OVrIzuPVZ
1mgdvhIPghf93qWOZDNLhPsibRuF_w9JwAxli_BFw-
JQA125u1mkaa9BrzGRWumHWkqbYJAN2BZbf1t3s-
UpEJszr6QBZTTVlDpRI89BcpJHFT2vxtiyqiXrc7NcwzNeWp4M7TRk-
LnLAeiATM3UsQ51_JtKWYrslFLIosZ7zolTgHd_jFBfiEdFBCHDJOLVvXHh_-
LhtfkqUZ1bf4aV6EBvZoZDPcHwEPCqsZbIXc5h0jwhUtL7aCAo3l8Xz0OUBRs3CLYrimr6kv
xUcyYTLD3-
owkNTFi3rrAiL9O_ZSlFIWWqjYpTyOSzuHrYlrLDLuneYLt2zK05wWqhXSmSIzCArJU2t56
JJKune48O03Vm0GrGs-DrllxaqAM-ck0gCZurmkmCbwcya0E98RzG8qVpjPM0-
YO4EESJmRboa7caTv9jZkP1vxVZIW1YSMyDRULPvfin0oJ46yeZRpYR8xSImDkvMZr9e6T
9g-
GoG80BUEE1pHQ99EMjpumTe9vPnJpTMBbR_PwypSPJhS2c6TS5tAeCvb8XPjMiiysspU-
1E3uVVTnsxbUIY9ylbDuM2OoctFA5Xe1zg-
2HMVHZ3TvDPm62NRyisFRA5Ob9uRETrJyItmnJZDgiVMqxAEgM3w5Dw7QWeWxix2z3
HqSSBp9o2mX-Xwg2Ri7od55qSjTcDP3Fee2kyNa2Xw-UvSfmZcJtg4xqxZS0wIWa-
D1ETPJeFbarQ1kKuoW3l-h6FnwE9C-aBHyh5MsIFfAam5kUDfvHJE4FKl-
ibZUiW3Ml684wJOP412JOJVf51lEQz__jz5Ua2AR2bUAq3-
6zHigIVQRVVQb3iFQAcV_xDkanpWfIJR1sabxHQPUbgQyAGUPdMKBhhqFwzKbOm0Aak
A-tVcJ3khAgUrFHBDObR_Z20cdxx8t4Tdf6IhlNqCGqv_K2g &
et=3 &
tcar=9 &
jsv=sdk_20190107_RC02-production-sdk_20220531_RC00 &
urll=4017 HTTP/1.1
[redacted]
x-afma-drt-v2-cookie:
CoABCnxEU0lEPUFBTy03cjRiX2lJZEFMRk5UNUpheXQzb3pjVF9rTk9nZERnNlNJZ3JZY
mxVLTR3bTcyd0JsZU90OFRXaUF2TEVyR25wOXRJcWJMZ1ROQV9QQ1BFUGV5bmVU
VVp6Y3lOXy14anlpX1VIMXNTeWdGTWdlZ3JRWVljGAE=
Host: googleads.g.doubleclick.net
Connection: Keep-Alive
Accept-Encoding: gzip

131. As with data that Google collects and saves using GA4F, the data that Google collects and saves using the Google Mobile Ads SDK (including AdMob, AdMob+, Ad Manager) is essentially unaffected by the user's WAA or sWAA settings.

3. Google Firebase Cloud Messaging

132. Firebase Cloud Messaging is a push notification system that can be integrated with Google Analytics. Google collects a variety of information via Firebase Cloud Messaging, including several types of events, parameters, and user properties.

133. As Google's Fourth Supplemental Response to Interrogatory No. 1 Section 2 on Data Logging Technical Details explains, the following events are sent to Google, along with debug messages:

- notification_receive: when the push notification was received by the app
- notification_foreground: when the push notification was received by the app while the app was in the foreground
- notification_open: when the user chose to open the notification[103]
- notification_dismiss: when the user chose to dismiss the notification

134. Google's Fourth Supplemental Response to Interrogatory No. 1 further explains that several event parameters are sent along with each of these FCM events, including:

- gcm_message_name: the name of the message in the FCM "Message Composer" UX
- gcm_message_time: the time at which the developer chose to broadcast push notifications. Alternatively, if the developer chose to use "device-local" time, message_time indicates a delivery time relative to each device's time zone.

[103] *See also* Answer ¶ 51.

- gcm_message_use_device_time: a flag which determines the interpretation of message_time.
- gcm_message_id: a unique ID for the message campaign
- gcm_sender_id: the sender ID corresponds to the developer's cloud project ID

135. As described in Appendix I, my testing proves that Google collects data from users' activity on non-Google apps by way of Firebase Cloud Messaging regardless of the user's WAA and sWAA setting states.

B. Google Has Saved WAA-off and sWAA-off Data Throughout the Class Period.

136. It is my opinion that Google, throughout the class period, has uniformly saved class members' WAA-off and sWAA-off data in numerous logs. Such data is identified as belonging to particular users through the various IDs Google saves and uses. Importantly, Google also associates such data with Google account holders' GAIA ID, which Google uses to determine the WAA and sWAA status of user data that Google collects and saves using GA4F and the Google Mobile Ads SDK. Moreover, in Google's Response to Request for Admission No. 25, Google admitted that "[a]t least one Google log contains one or more bits and/or fields that reliably shows whether specific event-level traffic was generated while WAA was off." Therefore, not only is Google saving WAA-off and sWAA-off data to class members' Google Accounts,[104] Google also marks some of the data as WAA-off or sWAA-off.

137. As I will discuss, within Google's non-GAIA logs, Google intermixes both WAA-on and sWAA-on data with WAA-off and sWAA-off data. Google has not accounted for all of the ways

[104] By "Google Account," with a capital "A," I am referring collectively to the trove of data that Google collects and saves regarding a user, including data that Google characterizes as "pseudonymous," because, as I explain below in Sections VII. G and I, WAA-off and sWAA-off data is saved with a multitude of Google identifiers that are linked to users.

it uses these data, especially within processes that rely on these stored data. However, based on my review of Google documents and produced data, it does not appear that Google treats the WAA-off and sWAA-off data in Google's non-GAIA logs any differently than it treats the WAA-on and sWAA-on data in those logs.

1. Google's Data Storage Overview

138. Google's data centers and cloud locations are located across the world.[105] These data centers and cloud locations store and process a surprising amount of user data. According to documentation that Google produced in this case, Google's "available storage capacity … can be measured in the order of [redacted]" (GOOG-RDGZ-00161364 at -367).

139. Google classifies user data into (A) "User Content (or 'explicitly provided data')" such as email, chat messages, email address and phone numbers and (B) "Logs (or 'implicitly collected data')," which includes "[i]nformation that Google generates about users, as a consequence of their interactions with Google services (e.g.: impressions, clicks, search queries, usage metrics, etc.)" (GOOG-RDGZ-00161364 at -374). Google further classifies the data it collects and stores in its logs as either "personal," (meaning explicitly tied to a GAIA ID), or "anonymous," which even Google recognizes as meaning explicitly tied to non-GAIA identifiers (GOOG-RDGZ-00161364 at -375).[106] "Personal" data tied to a user's GAIA ID are stored in "Personal logs (pLogs)" while data tied to a user's non-GAIA identifiers are stored in "Pseudonymous Logs" (GOOG-RDGZ-

[105] *Discover Our Data Center Locations,* Google Data Centers, https://www.google.ca/about/datacenters/locations/ (Last accessed February 15, 2023); *Cloud locations*, Google Cloud, https://cloud.google.com/about/locations#regions (Last accessed February 15, 2023).
[106] Even Google recognizes that "anonymous" data is at most "pseudonymous." The same documentation explains that "anonymous" data in Google's logs is tied to "pseudonymous cookie[s]" (GOOG-RDGZ-00161364 at -375).

00161364 at -410 and -411).[107] Google also stores user data in "Temporary Logs" where "there is not a hard requirement to distinguish between personal and anonymous logs" (GOOG-RDGZ-00161364 at -412).

140. Regardless of how Google internally classifies its logs, these logs store Google account holders' data. When, as here, the data is voluminous and detailed, purportedly pseudonymous data is linked to users (*see infra,* Sections VII.G, I).

a. Data Repositories for WAA-off and sWAA-off App-Activity Data

141. Google has not provided a complete list of Google logs and data storage repositories that store WAA-off or sWAA-off app-activity data from users. Based on the limited information Google produced, I have found several repositories that may store such data (this list is likely incomplete):

- **Sawmill Logs** – [redacted] (GOOG-RDGZ-00191895 at -897). Other Google documents explain that [redacted] (GOOG-RDGZ-00180626 at -627), and documents describe "Sawmill [as] [redacted] (GOOG-RDGZ-00027434 at -435). From Google's internal documents, it appears that Sawmill [redacted] (GOOG-RDGZ-00180220 at -222; GOOG-RDGZ-00042724 at -724; Ruemmler Tr. 218:9-15 [redacted]
- **Kansas/Oz and other "Planet-scale" storage** – Kansas an [redacted] (Oak Tr. 172:17-23). [redacted] (GOOG-RDGZ-

[107] Google's Third Supplemental Response to Interrogatory No. 1 notes in Section 4, Differentiated Logging, that "[p]seudonymous short-term logs have a [redacted] retention period[]" and "[t]hey are used to create aggregated event data logs for customer use."

00029866 at -866). (GOOG-RDGZ-00161364 at -398). Google's Fourth Supplemental Response to Interrogatory No. 1, Section 10 explains For example, GOOG-RDGZ-00175326 at -32 (GOOG-RDGZ-00175326 at -326 and -328).

- (GOOG-RDGZ-00181440 at -441)

- **MagicEye** – According to Google's internal documentation, Magic Eye is a (GOOG-RDGZ-00180626 at -627). (Fair Tr. 229:2-230:17). (GOOG-RDGZ-00180626 at -627). MagicEye (GOOG-RDGZ-00188356).

- .[109]

[108] "We've been collecting device-id-keyed Firebase conversion data, e.g., app open, in app purchase, and using UUAD pipeline to process the data for modeling and serving. These data has proven to be a positive impact on revenue…" (GOOG-RDGZ-00181440 at -441).
[109] *Link BigQuery to Firebase*, Google Firebase Help, https://support.google.com/firebase/answer/6318765 (Last accessed February 15, 2023).

[redacted] (Ganem Tr. 22:13-18). [redacted]

- [redacted] (GOOG-RDGZ-00193001 at -004). [redacted] (GOOG-RDGZ-00110367 at -372).

b. Footprints Data

142. Google also collects and saves app activity data in a repository called Footprints. According to David Monsees, Google's 30(b)(6) designee and Product Manager of Footprints, "Footprints is a back-end infrastructure for storing setting states and user data" (Monsees Tr. 90:11-13). Google uses Footprints for "storing, serving, analyzing, publishing, and syncing large amounts of user data," including "Chrome, Gmail, Android and many other clients" (GOOG-RDGZ-00185841 at -841).[110]

143. Footprints contains app activity data generated by signed-in users whose WAA and sWAA settings are on. According to Google's internal documentation, when a user has WAA turned on, Google collects and saves in Footprints "searches, Chrome history, and content [they] browse on the web and in apps" while on Google properties (GOOG-RDGZ-00025637 at -639). When a user also has sWAA-on, then Google also collects and saves in Footprints "Chrome browsing history and activity from websites and apps that use Google services" (GOOG-RDGZ-00025637 at -639

[110] In an internal document, Google explains that "Footprints is the primary, canonical storage for all Google activity data. My Activity is the UI for seeing, managing, and controlling this data" and "All activity-based personalization must be done using Footprints (or other primary sources like Location History), and not other data sources such as Logs/Sawmill" (GOOG-RDGZ-00118124). "Footprints uses Kansas as its primary storage backend. Kansas is implemented on top of BigTable" (GOOG-RDGZ-00087040 at -041). Another Google document explains that "My Activity is not a storage solution, it is a centralized transparency and control tool for our users. Most of the data stored in My Activity is managed by Footprints, so we can ensure data is deleted if the user deletes it. But Footprints itself is not a 'storage solution', it's just a management layer on top of data teams manage in Spanner, Kansas, logs, etc. As you know, no data in Footprints (per the underlying storage systems) can be accessed unless ACLs are granted, so "strict access" is part and parcel of the platform" (GOOG-RDGZ-00043813).

(emphasis omitted)). The sWAA setting affects only "FirebaseUserActions action reporting that gets logged *to Footprints*" (GOOG-RDGZ-00025637 at -639 (emphasis added)).

144. Because Google's policy is not to log sWAA-off data to Footprints, Google can pull the wool over its users' eyes, leaving them unaware that Google collects and saves their app activity data even when they have turned off WAA and sWAA. As Mr. Monsees testified, a user who "turned sWAA off" has "told Google, I don't want you to store this additional information" (Monsees Tr. 134:1-4). But if Google were to use the WAA-off and sWAA-off data to personalize the user's experience, the user might catch on. Mr. Monsees explained that "Footprints primarily serves as a personalization infrastructure" and that "there isn't a reason for [Google] . . . to store [sWAA-off] information in Footprints" (Monsees Tr. 133:18-134:7).[111]

145. As explained above in Section VI.B, in connection with Narnia 2, Google began making some data visible in a user-facing dashboard called My Activity; some of this data is also available in a tool called Google Takeout. The data that Google makes visible to users through these tools is drawn from Footprints. Greg Fair, a former Senior Product Manager on Google's privacy team, testified that Footprints "is synonymous, roughly, for My Activity" (Fair Tr. 104:21-105:7). Documents that Google produced in this litigation similarly explain that "[a] good rule-of-thumb is that Footprints data maps to My Activity" (GOOG-RDGZ-00180626 at -627). Google describes My Activity as "[u]ser-facing transparency, control, and consents," (GOOG-RDGZ-00020110 at -124) but the truth is that it includes data from one source—Footprints.

146. I have not found documentation or testimony indicating that data stored elsewhere within Google's vast storage systems are made available to end users. To the best of my knowledge,

[111] Mr. Monsees' testimony is further supported by Greg Fair's testimony: "Q…So I have WAA off or WAA disabled or paused. That essentially puts the big cap on the Footprints jar and prevents any information from being written there and associated with my GAIA account; correct? A. That's a reasonable way of expressing it, yeah" (Fair Tr. 118:4-10).

Google allows users to see their data only to the extent it is collected and saved in Footprints; Google does not make data that it collected and saved in other systems available to its users, meaning that users have no way to see their data that Google has saved when WAA or sWAA are turned off.

c. Google's Storage of Users' WAA and sWAA Settings and Other User and Device Information Storage

147. Google also collects and saves users' WAA and sWAA settings on both user devices and Google's servers. Google collects and stores users' WAA and sWAA status in several locations. David Monsees, Google's 30(b)(6) designee and Product Manager for Footprints, described Footprints as the "source of truth"[112] for a user's WAA and sWAA status, and he also testified that a "mirror" of the WAA and sWAA status as recorded in Footprints is also saved on the user's device.[113] Google also saves a copy of users' WAA and sWAA settings in Magic Eye, along with substantial other information.[114] According to Mr. Monsees, Google's Footprints team also provides other teams with "various systems" they can use to "read the WAA signal," which "are controlled within the scope of Footprints infrastructure" (Monsees Tr. 90:4-8).

[112] "That source of truth for the state of WAA is stored in Footprints -" (Monsees Tr. 89:2-6); "Footprints, I mentioned in my previous answer, is the source of truth. And to clarify, what I mean is that the – the official state of the Web and App Activity setting" (Monsees Tr. 89:13-20); The "source of truth" is "on the server as where the – the primary source of the settings would live" (Monsees Tr. 99:18-21); "Q…you are still responsible for Footprints, which you do agree at least as it is responsible for the initial account lookup that tells you whether a user has sWAA on or sWAA off; is that correct? A. That's correct, Footprints is the source of truth for the state of the settings" (Monsees Tr. 122:13-22); "There's the Footprints activity control service, that's what's going to store for David's Google account at this date, time, sWAA was turned on or sWAA was turned off. That's going to store the record of setting states and setting state history. This is the source of truth . . ." (Monsees Tr. 148:16-23).

[113] "[redacted] onsees Tr. 161:10-18).

[114] "[redacted] (Monsees Tr. 176:4-7) a[redacted] (Monsees Tr. 314:14-19); *see also* GOOG-RDGZ-00188356 at -359.

148. In its Response to Interrogatory No. 13, Google also explains that it maintains a dashboard called "'My Activity Metrics,'" which "provides certain measurements of Google account interactions with the Web & App Activity setting," as well as the "'Web & App Activity Log,' which tracks Web & App Activity on-and-off events for all Google Account IDs on an individual level."

149. Google produced the WAA and sWAA status of the named Plaintiffs' Google accounts along with the date and time. For example, GOOG-RDGZ-00013598 shows that the WAA setting associated with [redacted] was "on" beginning on August 24, 2018 and then toggled off and on a few times in 2019 and 2020; WAA was then turned off ("paused") on July 29, 2020, and it has remained off since. GOOG-RDGZ-00013598.0001 shows that the sWAA setting associated with the same account was "on" between August 24, 2018 and July 7, 2019, and has been turned off since that time. Across all the produced WAA/sWAA records for the Plaintiffs (GOOG-RDGZ-00013598 to GOOG-RDGZ-00013641; GOOG-RDGZ-00124316 to GOOG-RDGZ-00124317; and GOOG-RDGZ-00124327 to GOOG-RDGZ-00124328), the earliest available WAA status date was March 1, 2006 (GOOG-RDGZ-00013632), and the earliest available sWAA status date was January 13, 2015 (GOOG-RDGZ-00013633.0001).

150. A summary of the WAA and sWAA settings of Sal Cataldo, Susan Harvey and Anibal Rodriguez is shown in **Appendix A**. Each tab in Appendix A lists the Plaintiff's Google account, recovery email and SMS phone number, as well as the produced WAA and sWAA records.

151. Google's records of WAA and sWAA status are accurate. Consultants working at my direction performed certain data testing using test accounts,[115] which included toggling WAA and sWAA on and off.

152. Google has also produced the Google Subscriber Information associated with the named Plaintiffs' Google accounts, which includes GAIA, Name, e-mail, phone number, account creation date, IP address at the time of account creation, and date/time and IP address of the user every time the user signed-into Google (GOOG-RDGZ-00013554 to GOOG-RDGZ-00013597; GOOG-RDGZ-00124313 to GOOG-RDGZ-00124315; GOOG-RDGZ-00124318 to GOOG-RDGZ-00124326). Google appears to retain Google Subscriber Information records regarding dates and times at which the user signed into Google for nine months. *See* GOOG-RDGZ-00013554 (Google Subscriber Information for [redacted] generated on February 17, 2021, including sign-in events dating back to May 17, 2020, and no further).

153. The Google Subscriber Information can also be found in Google Takeout. For example, I have included Google Subscriber Information for the test account "phoenixfire202205@gmail.com" in Exhibit B-3, file "phoenixfire202205.SubscriberInfo.html." This record includes the GAIA ID, date, and time of account creation, Contact e-mail address, and a table of IP activities. This IP activities table includes user Login and Logout Timestamp (including date and time), IP address (IPv4 and IPv6) and Raw User Agent (which identifies the device, device model, operating system and operating system version. If the sign-in activity was from a web browser, the browser and browser version are included). In Exhibit B-3, file "Profile.json" shows the user's given name, family name, email and gender.

[115] This process is described in more detail in Appendix G.

154. Google Takeout also includes a list of user devices associated with a GAIA ID. For example, Exhibit B-3, file "Devices – A list of devices (i.e. Nest, Pixel, iPh.csv," includes devices associated with the test account "phoenixfire202205@gmail.com." As reflected in the Google Takeout file, this account is associated with four devices, two of which are mobile devices (one Android, another iOS), and two of which are desktop devices (one Windows, another Mac). The Android device is a Samsung phone with device model SM-G780G, and operating system version 12. The device was last accessed in the US. The iOS device is an iPhone SE (3rd generation) with device model iPhone14,6 and operating system version 15.5. The device was last accessed in the US. The Google Subscriber Information in Google Takeout is accurate.

155. For Android devices, Google also keeps detailed Android device configuration service data. For example, in Exhibit B-3, file "Device-4514249733518502807.html" includes Android ID, IMEI (International Mobile Equipment Identity – a unique 15-digit code that identifies a mobile phone), device serial number, location, time zone, device attributes (including hardware, model, brand, manufacturer, device type, radio firmware version, touch screen type, keyboard type, screen density/height/width, etc.). This device file also contains a multitude of other device hardware and software information. This information is accurate.

156. Google also maintains a record of user activities on Google's owned & operated products (e.g., Gmail, Search, Photo, Maps, YouTube, etc.). For example, in Exhibit B-3, file "Activities - A list of Google services accessed by.csv", includes the device type (i.e., mobile) and operating system (i.e., Android or iOS), version, and app used as determined from the User Agent String, and the date and time of access and IP address (IPv4 and IPv6).

157. Google also stores a list of apps downloaded and installed on Android devices along with the date and time of first installation and last update. For example, in Exhibit B-3, files within the

Google Play Store folder, show numerous app installation records. An example for the app "Hill Climb Racing" is shown in the figure below.

2. Google's Storage of WAA-off and sWAA-off GA4F Data

a. Analytics Data Consent Check

158. Google does not dispute that it saves app analytics data with Google identifiers, even when a user has WAA or sWAA turned off; the WAA and sWAA settings affect only which Google identifiers are used, and where the data is saved. In this section, I will explain how Google saves WAA-off and sWAA-off GA4F data.

159. As explained above in Section VII.A.1, Google collects GA4F data in HitBundles. [redacted] (Google's 4th Supp. Resp. to Interrog. No. 1, § 4).

160. [redacted]

[116] Jesse Savage, *Better Understand and Reach Your Customers with New Cross Device Capabilities in Google Analytics*, https://analytics.googleblog.com/2018/07/cross-device-capabilities-mktg.html (Last accessed on March 20, 2023).

[redacted] (Stone Tr. 35:3-6). [redacted]

161. [redacted] (Google's 4th Supp. Resp. to Interrog. No. 1, § 4). [redacted] (Google's 4th Supp. Resp. to Interrog. No. 1, § 4). [redacted] (Google's 4th Supp. Resp. to Interrog. No. 1, § 4).

162. [redacted],[117] [redacted] (GOOG-RDGZ-00050748 at -748 [redacted] GOOG-RDGZ-00178445 at -447)). [redacted] (GOOG-RDGZ-00050748 at -748). [redacted]

[117] "Mobile definition of signed in/ out - For android, signed in means device level sign in" (GOOG-RDGZ-00200800 at -975).

[redacted]

163. [redacted] (Ganem Tr. 66:22-67:3). [redacted] (GOOG-RDGZ-00047495 at -499 and GOOG-RDGZ-00181440 at -445). [redacted]

[redacted] (GOOG-RDGZ-00181440 at -450).

[redacted] (Monsees Tr. 107:19-25).

produced (GOOG-RDGZ-00047495 at -499):

164. (GOOG-RDGZ-00200800 at -975; *see also* GOOG-RDGZ-00181141 at -145), (Ganem Tr. 50:17-20).

165. (GOOG-RDGZ-00047495 at -500).

[redacted][120] [redacted]

[redacted]

[redacted]

[redacted]

[redacted].[121] [redacted]

[redacted]

[redacted]

[redacted]

[redacted] (GOOG-RDGZ-00047495 at -500):

[redacted]

[120] [redacted] (GOOG-RDGZ-00181141 at -141).

[121] If IDFA is not available, then Google cannot look up the user's setting state, and it associates the data with non-GAIA identifiers (Ganem Tr. 72:4-73:3).

[122] "The status of both the Web and App Activity and Supplemental Web and App Activity setting as it applies to Google Analytics isn't forced in the Footprints infrastructure, and I believe that Google Analytics systems do look up that state from Footprints" (Monsees Tr. 107:19-25).

166. As explained above in Section VII.A.1 and as Google admits, the WAA and sWAA settings do not affect whether Google collects GA4F data; they affect whether Google saves the data alongside the user's GAIA ID after performing the consent check (Google's 4th Supp. Resp. to Interrog. No. 1). If the user's WAA and sWAA settings are on, Google saves data it collects via GA4F with the user's GAIA ID, and makes it appear in My Activity for users to view. But if the user's WAA and/or sWAA settings are off, Google saves the data it collects via GA4F with the user's other Google identifiers (e.g., app instance id, ADID), rather than with the GAIA ID. WAA-off and sWAA-off GA4F data do not appear in My Activity, and therefore users are unable to review this data.

167. Google represents that the aforementioned consent checks implicate WAA, sWAA, GAIA Ads Personalization (GAP)[123], and a supplemental checkbox under the GAP control (NAC – New Ads Control) (Google's 4th Supp. Resp. to Interrog. No. 1, § 4). Regardless of the user's settings, Google uses GA4F to collect and save the data in a log with non-GAIA identifiers (e.g., ADID, IDFA, app instance id — most of which are issued by Google); if all of the aforementioned settings are enabled, Google also uses GA4F to collect and save the very same data in another log, with GAIA (Ganem Tr. 140:21-141:2). It is important to note that if the developer of a single app on a user's device enables Google Signals, that user's device ID (i.e., ADID or IDFA) will be linked to their GAIA ID, creating a link that persists even for apps that do not enable Google Signals.

168. In his 30(b)(6) deposition, Steve Ganem testified, "Google Analytics AppMeasurement logs, pseudonymous logs, have fields for IDFA and ADID." (Ganem Tr. 252:12-15). Steve Ganem discussed how these events and third-party app data is first written in, "I believe it's the app measurement logs" (Ganem Tr. 42:11-12).

[123] "Gaia Ads Personalization A new feature (on by default for new accounts) allows users to choose to apply their account-level ads settings off of Google" (GOOG-RDGZ-00204257 at -329).

169. Google documentation indicates that [redacted] and [redacted][24] status are stored in analytics logs by the analytics front end server GOLFE (GOOG-RDGZ-00207976 at -977). Prior to March 2022, GA4 also stored IP addresses.[125]

170. A user can also be signed out of Google. In this case, all collected data are stored with a user's non-GAIA Google identifiers.[126] Regardless of user or app developer settings,[127] a copy of the user's app analytics data is stored by Google in the user's Google Account.

b. Analytics Data Logging

171. Google saves data collected via GA4F in various logs and other data stores, including alongside additional data from other sources such as AdMob. According to Google, the "pipeline" for GA4F data generally includes five components: [redacted] Google's 4th Supp. Resp. to Interrog. No. 1, § 9). [redacted] (Google's 4th Supp. Resp. to Interrog. No. 1, § 9). [redacted]

[124] On Android devices, users previously had a control setting called "Opt out of Ads Personalization" (OOOAP).
[125] Russell Ketchum, *Prepare for the Future with Google Analytics*, Google Marketing Platform, https://blog.google/products/marketingplatform/analytics/prepare-for-future-with-google-analytics-4/ (Last accessed February 15, 2023).
[126] As explained by Steve Ganem in his deposition, "the person, has a second Android phone, but you're not signed in on it, then the data that is collected via GA for Firebase could not be associated with your Google account that has sWAA off, and would be treated as a pseudonymous profile and subject to device level settings such as LIT and Ooo app (Phonetic), could be used for ads personalization in the pseudonymous space" (Ganem Tr. 284:12-19).
[127] The only exception is if the app developer does not use Google Analytics products. However, since a user typically has many apps installed on a device, the probability that none of the installed apps use Google Analytics is very low, as I will discuss later in the report.

[redacted] (Google's 4th Supp. Resp. to Interrog. No. 1, § 9). [redacted] (Google's 4th Supp. Resp. to Interrog. No. 1, § 9). [redacted] (Google's 4th Supp. Resp. to Interrog. No. 1, § 9). In the final stage, a "query serving component" reads from aggregates and "serve[s] responses to [the] front end or API[s]" (Google's 4th Supp. Resp. to Interrog. No. 1, § 9). Google uses something called "blobstore as backup storage for baseview and aggregates data" (Google's 4th Supp. Resp. to Interrog. No. 1, § 9).

172. Google also saves GA4F user data in many repositories other than baseview. There are so many data sources that Google has asserted that "it is not practical" to even list them all (Google's Resp. to Interrog. No. 14). And indeed, Google has refused to provide a full list of logs and data stores that include data that Google collects and saves using GA4F. However, other discovery provides some information about these logs and repositories.

173. In Google's Fourth Supplemental Response to Interrogatory No. 1, Section 10, Google represents that the [redacted]

174. Google has provided some information regarding the retention periods of its various logs, even though it has not identified those logs. [redacted] (Google's 4th Supp. Resp. to Interrog. No. 1, § 11). Aside from GOOG-RDGZ-00071768, which contains

some of the fields in what appears to be a GA4F collection log, Google has not produced a list of all fields stored in these analytics logs nor description of the stored data.

175. Google also saves GA4F user data, including from WAA-off and sWAA-off users, in many data repositories that Google has not identified in its Interrogatory responses. For example, one document that Google produced in this case indicates that Google [redacted] (GOOG-RDGZ-0017742 at -747). [redacted] (GOOG-RDGZ-00177538 at -539 and -540[128]; GOOG-RDGZ-00180278 at -279). [redacted] (GOOG-RDGZ-00180278 at -279).

176. [redacted] (GOOG-RDGZ-00177433 at -446). [redacted] (Ganem Decl. (February 22, 2023) ¶ 2). [redacted]

[128] *See also* GOOG-RDGZ-00200565 at -579 (On User Store: [redacted]

[redacted]

177. [redacted] (Ganem Tr. 164:5-6). [redacted] (Ganem Tr. 164:5-6, 164:14-15). [redacted]

(Ganem Tr. 307:4-14).

c. Plaintiff and Test Device Analytics Data Analysis

178. As a part of my investigation, I have observed Google's extensive collection and saving of WAA-off and sWAA-off GA4F data in its Analytics logs and other repositories. This part of my investigation involved two components. First, the named Plaintiffs provided Google identifiers obtained from their Android devices to Google, allowing Google to search for and produce their data from within Google's Analytics storage infrastructure. Second, I used four test devices to perform certain activity on apps, as described in Appendix G. Non-GAIA identifiers associated with these devices and their apps as well as signed-in Google account emails were provided to Google. Using the submitted non-GAIA identifiers from Plaintiffs' devices and test devices, Google produced GA4F data from an Analytics collection log (for the four test devices) and a downstream Baseview store (for the test devices and named Plaintiffs' devices). Google also produced a set of GAIA GA4F data from the Analytics collection log.

179. In Appendix K, I have included a small sample of the data that Google produced, including WAA-off and sWAA-off events from each of the named Plaintiffs' devices and test devices. This

Appendix includes four event entries from the collection [redacted] log and seven event entries from the Baseview store. As these events show and as I discuss in detail below, Google stores extensive WAA-off and sWAA-off data in its various logs and data repositories. Google collects and saves quite detailed information about these events, often including a variety of Google identifiers and other identifying information such as email, name, and phone number. The volume of the data that Google collects is telling. The data for these 11 event entries spans *more than 160 pages*, as reflected in Appendix K—*single spaced*, with many event parameters packed into a single line for some of the events, and with incomplete data for two of the event entries (Google failed to produce the full records of those events). Google collects and saves these extensive WAA-off and sWAA-off data in non-GAIA logs, intermixed with WAA-on and sWAA-on data, with no apparent distinction in the type of data stored.

Baseview Data

180. The Baseview data Google produced from Plaintiffs' devices consists of Android app analytics data located using ADIDs extracted from the named Plaintiffs' devices (GOOG-RDGZ-00071766; GOOG-RDGZ-00071767). During this data search process, Google agreed to use only Android ADIDs for search. Since Plaintiff Julian Santiago had an iPhone, his identifiers (e.g., IDFA) were not submitted for search. The produced files are quite large. GOOG-RDGZ-00071766 contains 2.83 Gb and GOOG-RDGZ-00071767 contains 1.35 Gb of user data, spanning October 16, 2021 to December 19, 2021. A small subset of the produced data from Sal Cataldo, Susan Harvey and Anibal Rodriguez is included in **Appendices B.1 and B.2** of this report.

181. As described in Appendix G, I directed the consultants working with me to generate test data on two Android and two iOS devices, while signed-in and with either WAA-off (and sWAA-off), WAA-on and sWAA-off, or WAA-on and sWAA-on, in order to observe how setting states

affect the way that Google collects and saves app activity data.[129] On February 23, 2023, Google produced additional Baseview data generated from the four test devices, which it searched for and collected using the ADID or IDFA from these devices. The produced file contains 842 Mb of user data spanning two weeks between January 13, 2023, and January 27, 2023. A small subset of the produced data is included in **Appendix B.3** of this report.

182. On each of these Plaintiff and test devices, the user was signed into a Google account during the period for which Google produced data. The signed-in Google account for each of the test devices is listed in Appendix G. For the Plaintiffs, I understand that Sal Cataldo was signed into his [redacted] account (Cataldo Tr. 88:17-89:10); Susan Harvey was signed into her [redacted] account (Harvey Tr. 114:22-23); and Anibal Rodriguez was signed into his [redacted] (Rodriguez Tr. 61:4-5). As shown in Appendix A, all three Plaintiffs' signed-in accounts had WAA and sWAA turned off when the Baseview data was generated.

183. From the timestamps in Google's Analytics Baseview records and WAA and sWAA status records, it is straightforward to determine a user's WAA and sWAA status when the user generated the event and the WAA and sWAA status of the user by the time the event reaches Google. *See* Appendix G.

184. The Baseview records in Appendix B.3 confirm that Google collects and saves GA4F data in non-GAIA logs regardless of the user's WAA and sWAA state. In all possible setting combinations (WAA-off, sWAA-off; WAA-on, sWAA-off; and WAA-on, WAA-on), Google uses GA4F to collect and save user data in these logs. Google also collects and saves the same types of user data in these logs, regardless of these user settings.

[129] For one of the iPhones, the WAA and sWAA settings of the signed-in Google account were off for the entire duration of the test.

185. The produced data also supports my understanding that app instance id is unique for each app on a device. As discussed in Appendix G, the "App and Instance ID" tabs in Appendices B.1-B.3 show a complete list of apps and their app instance ids in the produced records. For example, some of the apps, such as Uber, are installed on multiple people's devices. However, each instance of the Uber installation has a unique app instance id. As I discussed in Appendix G, Google also stores a user_id field in Baseview records. Based on my analysis, this user_id is unique for each app on a device and identifies user data in a similar way as the "app instance id". Google's Baseview records contain *thousands* of fields, amounting to a highly detailed account of the user's activity on non-Google apps, all of which is associated with the user's Google IDs. I have observed the following categories of WAA-off and sWAA-off data in the produced Baseview records.

ScreenView

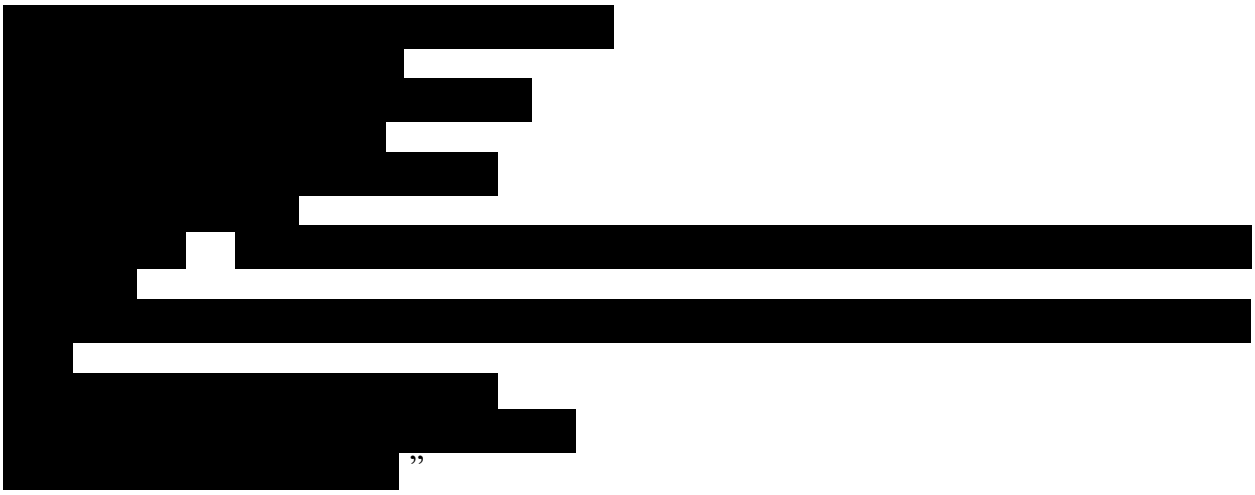
186. As discussed earlier, GA4F tracks screen_view events. Some of the values in the "screen_name" field are: "JobDetailFragment," "RegistrationActivity," "LoginActivity," "PurchaseActivity," "CheckoutFragment," "CartActivity," "ShopListActivity," and "RewardsActivity."

Other Content

187. Google sends not only the name of the screen, but also detailed information about the screen—and therefore the user's activities and proclivities.

188. For example, while both WAA and sWAA were turned off, the Android 1 test device used the Washington Post app and visited a sensitive article, regarding how to determine whether the frequency and color of a person's bowel movements are indicative of a health problem. Google collected and saved in Baseview data reflecting this sensitive, medical activity, along with the user's email address (phoenixfire202205@gmail.com), ADID, app instance id, latitude/longitude

and other user, device and app information (event 1819 in the original February 23, 2023 production, corresponding to Appendix B.3 event 1818):



”

189. The Android 1 test device also visited a Washington Post article that described smartphone cameras’ failure to accurately capture dark skin and compared how well Apple, Samsung, and Google devices performed. From Google’s Baseview logs, this activity can be recreated exactly (event 1684 in the original February 23, 2023 production, corresponding to Appendix B.3 event 1683). Google again stored this event with the user’s email address (phoenixfire202205@gmail.com), ADID, app instance id, latitude/longitude and other user, device and app information.

“content_author”: “chris velazco”

Identifiers in Non-GAIA Logs

190. While Google claims that non-GAIA data is not reasonably linkable to a user,[130] the reality is that Google collects and saves WAA-off and sWAA-off data with identifiers that tie the data to a person, including name, e-mail, phone number, and Google identifiers.

191. Take another example, Plaintiff Anibal Rodriguez's WAA-off and sWAA-off data. For Mr. Rodriguez, Google searched Baseview for GA4F data associated with his ADID.[131] In the following collection of data from Baseview (GOOG-RDGZ-00071766; GOOG-RDGZ-00071767), I [redacted] A small subset of the app analytics information Google stores is shown in the table below, taken from GOOG-RDGZ-00071767. The data in this log is anything but anonymous.

[130] I explain below in Section VII.G more generally how WAA-OFF and sWAA-OFF data are linked to users.

[131] [redacted]

[132] The same name, e-mail and phone number are in Anibal Rodriguez's GAIA record. *See* Appendix A.

[133] "Career Karma is a community of peers, mentors and coaches that will help you land a dream career in Tech. You never pay a dime. The only cost is to help people behind you. In our app, you will meet people who are just starting out and people who are several stages ahead of you. No prior experience is needed. We will send you a free coding course to get started." *Career Karma*, Google Play, https://play.google.com/store/apps/details?id=com.careerkarma.chat&hl=en_US&gl=US (Last accessed February 15, 2023).


a
ssthrough"
: "no"
}

192. I found similar data in the non-GAIA logs associated with Susan Harvey's device. Like for Mr. Rodriguez, Google searched Baseview for Ms. Harvey's ADID and produced the resulting data. In that non-GAIA data, I [redacted] small subset of the app analytics information Google stores is shown in the table below, taken from GOOG-RDGZ-00071767.

[redacted]

[134] The same name and phone number are in Susan Harvey's GAIA record. *See* Appendix A.
[135] "Download the mobile app & discover how the possibilities are even more beautiful. Find your favorite makeup, skincare & haircare products—plus shade match and color swatch your favorite makeup and haircare in GLAMlab®, our virtual beauty try-on experience. Then, check your Ultamate Rewards account & redeem points anytime, anywhere." *Ulta Beauty: Makeup & Skincare*, Google Play, https://play.google.com/store/apps/details?id=com.ulta&hl=en_US&gl=US (Last accessed February 15, 2023).

193. Google produced similarly voluminous Baseview data associated with test accounts ("test1.rodriguez@gmail.com" and "phoenixfire202205@gmail.com"), regarding activity on non-Google apps when WAA and sWAA were turned off.

Sign-in Status in Logs

194. The produced Baseview data contains several fields that indicate whether a user is signed in with Google and with non-Google apps. These include:

- signed_in_with_gaia: which indicates "whether the end user has signed in with Gaia" (GOOG-RDGZ-00174751 at -760). Steve Ganem testified that "there is a single bit

indicating whether … the user was signed in at the time the event was transmitted" (Ganem Tr. 243:16-18).

- signed_in_with_user_id: which "is an indicator for whether an event is signed in with user id or not" (GOOG-RDGZ-00177895 at -901). This data is also "added to AggregateRecord" (GOOG-RDGZ-00177895 at -901).

LAT/ATT Status in Log

195. As shown in Appendices B.1-B.3, GA4F Baseview contains fields that denote whether the user has enabled settings called "Limited Ad Tracking" or "App Tracking Transparency." These fields are "is_limited_ad_tracking" and "att_status."

Revenue

196. The produced Baseview data contain several revenue-related fields, including "event_params:key:ad_revenue," "third_party_ad_revenue," "ecommerce:event_revenue," "ecommerce: product_revenue," "ecommerce:lifetime_revenue," and "impression_ltv_revenue."

Demographics and Interest Profiles

197. The produced Baseview data, including data in non-GAIA logs, also contains demographics (age, country, gender) and user interest profile information, for example: "interest_id," which is "The IDs of the user's affinity interests" (GOOG-RDGZ-00082467 at -472); "inmarket_interest_id," which is "The name of the in-market audience (the group of people who are actively searching and comparing [] product or service)" (GOOG-RDGZ-00082467 at –471 and -472); and "branding_interest_id," which lists a series of code that represents a user's brand interest. The field "branding_interest_id can be directly read from baseview for audience evaluation. Audience BE [backend] does that currently" (GOOG-RDGZ-00111844 at -844).

Collection Log Data

198. Google's counsel initially represented that "We cannot produce GA4F collection log data using a deviceID because the deviceID is encrypted in a way that makes it prohibitively difficult to decrypt" (Email from Eduardo Santacana on March 1, 2022). As a result, Google did not produce Plaintiffs' Analytics data from GA4F collection logs. However, on January 20, 2023 and January 31, 2023, Google did produce test data stored in Google's GA4F collection log, called "[redacted]." As mentioned, these data originated from four test devices. I describe these tests and test results in detail in **Appendices G, H.1 and H.2**.

199. The test results further support my opinion that Google stores WAA-off and sWAA-off app analytics data along with a multitude of identifying information discussed above. Such data can be retrieved by class members' device identifiers (e.g., ADID and IDFA). The data also contains other identifiers such as a hashed version of Google's app instance id, which can also be used to retrieve user data.

200. Google's production of data from its GA4F collection log further shows that Google collects and saves WAA-off and sWAA-off data with information like Gmail addresses, which are associated with a GAIA ID. If any piece of identifying information (including, but by no means limited to a Gmail account) is saved in one of the user's non-GAIA records, then *all* data associated with the same non-GAIA identifiers (e.g., ADID/IDFA, app instance id, etc.) uniquely identify the user.

201. As discussed in Appendices H.1 and H.2, Google's production of data from its GA4F collection logs also shows that Google collects and saves GA4F data in non-GAIA logs associated with device IDs in all possible WAA and sWAA setting combinations (WAA-off, sWAA-off;

WAA-on, sWAA-off; WAA-on, sWAA-on). The types of stored data are also the same regardless of these user settings.

202. Google's January 31, 2023 production of data from its GA4F collection log also shows that Google saves GA4F data in non-GAIA logs using substantially the same structure and content as the data it saves in non-GAIA logs. Because Google stores a copy of "consented data" in both GAIA and non-GAIA logs, the timestamps, identifiers, and data stored in both types of logs make GAIA and non-GAIA data and ID joining straightforward. This means that if a user had WAA on or sWAA on for a time during the class period, their WAA-on and sWAA-on data links their non-GAIA identifiers to their GAIA IDs. Effectively, linking GAIA ID to a single non-GAIA record containing ADID or IDFA links all of the user's data with the same ADID or IDFA to that GAIA ID. The same can be said about app instance id and any other Google identifier that uniquely identifies an instance of an app.

3. Google's Storage of WAA-off and sWAA-off App Ads Data

a. App Ads Data Logging

203. Like with analytics data, data collected by way of Google's app ads products are stored in Google logs irrespective of the user's WAA or sWAA status. The WAA and sWAA settings affect only which Google identifiers are used, and where the data is saved.

204. As discussed in Section VII.A.2, when a user is signed into Google and has WAA or sWAA turned off, app ads data arrives at Google with both GAIA and non-GAIA identifiers. After the consent check, Google saves the data in long-term logs and the data may also be processed downstream through Google's ad stack.

205. Like analytics data, WAA and sWAA merely control whether app activity data from non-Google apps is stored with a user's GAIA ID in Google logs. Specifically, when WAA/sWAA is on, the data may be stored with a user's GAIA ID; when WAA/sWAA is off, the data is stored

with a user's non-GAIA IDs.[136] Google's Supplemental Response to Interrogatory No. 23 explains: "When a user is logged into their Google Account and has turned WAA and/or sWAA off, any data that is collected by the Google Mobile Ads SDK is logged against pseudonymous identifiers."

206. Google uses bits within ads logs to track the WAA and sWAA status of event-level data. Google's Supplemental Response to Interrogatory No. 17 explains: "Google identified a log called [redacted] that indicates WAA and sWAA status alongside ad interactions, e.g., views and clicks, on App Campaigns designated app-install campaigns." Google relatedly admitted in its Response to Request for Admission No. 25 that "[a]t least one Google log contains one or more bits and/or fields that reliably shows whether specific event-level traffic was generated while WAA was off." Therefore, not only is Google saving WAA-off and sWAA-off data to class members' Google Accounts (both before and after the consent check) Google also marks some of the data as WAA-off or sWAA-off.

207. On February 7, 2023, Google's counsel provided a list of "AdMob Logs" "identified through a reasonably diligent investigation of the logs AdMob may log ad interaction data to from devices used by users whose Google accounts may have had WAA or sWAA turned off at the time of the data was generated" (Feb. 6, 2023 Email from E. Santacana, Re: Rodriguez: Letter Brief on 9th Set of RFPs and Open Requests). This list of logs, shown below, includes both non-GAIA logs and personal logs. My understanding, based on reviewing Google's internal documentation, is that personal logs contain users' GAIA IDs (GOOG-RDGZ-00185868). Furthermore, Google's

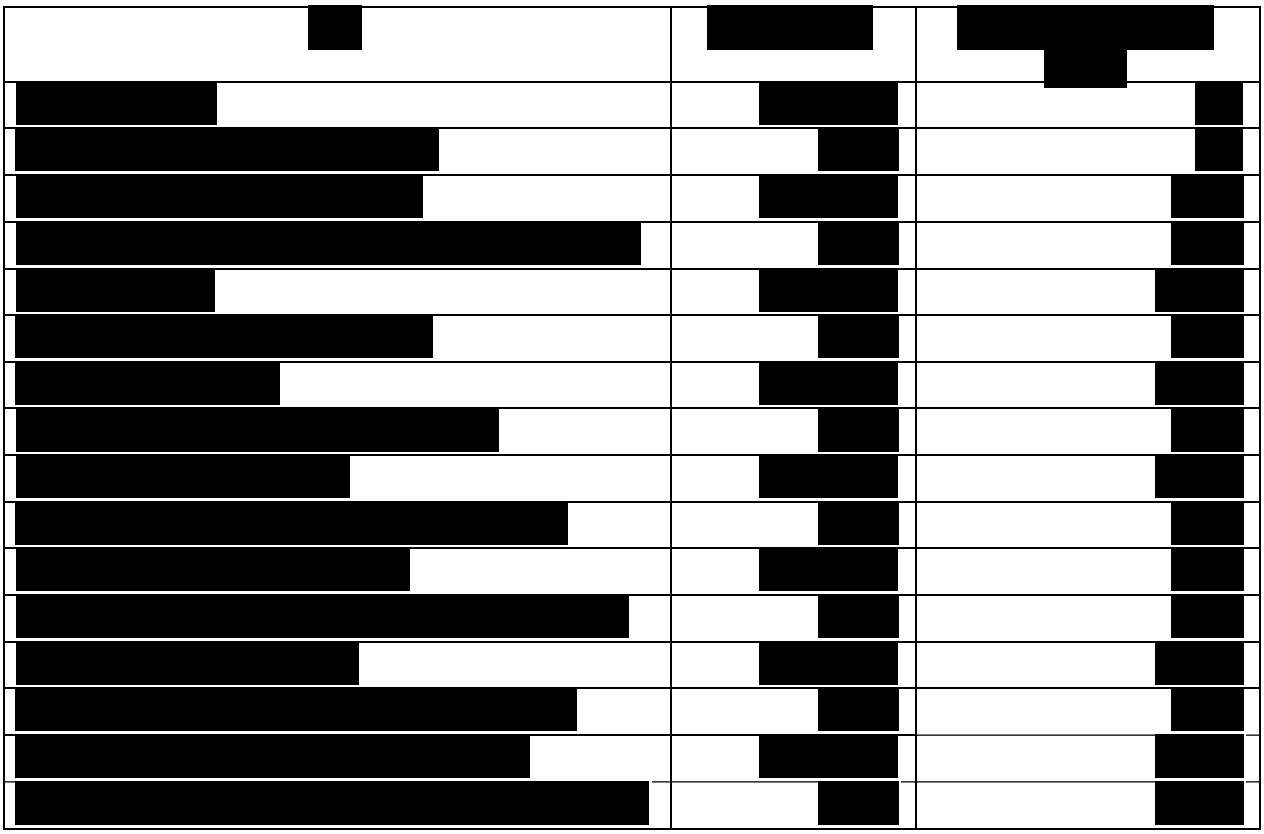
[136] Google states in Section 3 its Third Supplemental Response to Interrogatory No. 1, titled Consent Checks and Technical Barriers to Joining, that "[e]ach of WAA, sWAA, GAP, and NAC are account-level Web & App Activity and Ads Personalization controls. If sWAA, GAP, and NAC are all turned on, the result of the consent check is that the data can be tied to a user's Google account in what is known as 'GAIA space.' If any of these controls are off, then the data isn't joined to a user's Google account, and therefore not logged in 'GAIA space.'"

counsel's email stated that "we queried the logs' fields with the relevant terms that we know tend to be used for a WAA or sWAA bit based on prior discovery in this case" (Feb. 6, 2023 Email from E. Santacana, Re: Rodriguez: Letter Brief on 9th Set of RFPs and Open Requests). Thus, these logs contain WAA/sWAA bits that indicate a users' WAA and sWAA status, if the fields are populated with values.

208. A month before this report was due, Google finally provided field names for these 16 logs but without any description for any of the fields.[137] On March 20, 2023, Google formally produced the field names in GOOG-RDGZ-00211106, again without any description for any of the fields. Google also did not produce any data from any of these logs. The number of fields produced for each log is shown in the table below. While some of the logs contain tens of thousands of fields, there are likely even more fields that Google did not produce. Google represented that "the list of fields was obtained by querying a sampled field log that contains 1% of all entries from the underlying log" (Mar. 3, 2023 Email from E. Santacana, Re: Rodriguez: Letter Brief on 9th Set of RFPs and Open Requests). This representation indicates to me that the fields that did not happen

[137] HC-AEO Rodriguez - Fields in AdMob Logs (WFG to Susman Feb 22) HC-AEO.xlsx

to appear in the 1% of sampled entries were not produced. On the other hand, the fields that were produced are fields that are currently actively logging data.



209. The expansive list of fields sheds light on the impressive scope of Google's collection and storage of data.

210. Google's 30(b)(6) designee, Belinda Langner[138] testified that "The Google Ads systems can choose to display an ad to a specific user like we talked about within an app, okay? That user can then click on that ad. That information is all logged" (Langner Tr. 156:14-18). Internal Google documentation shows that "If the app has installed the Google Mobile Ads SDK, we collect ads log information related to app usage and ad impressions, tied to the device's Advertising ID, including: IP address, Timestamp, Encoded advertising ID, SDK version, Information about the

[138] Belinda Langner is a product manager responsible for app campaigns (Langner Tr. 20:9-25). Langner has been "involved in the development of app campaigns since at least 2015" (Langner Tr. 26:11-17).

app (version, topics, etc.), Information about the ad content served (advertisement, campaign ID, etc.) and Information about the device (app/OS/hardware version, location, wireless speed, etc.)" (GOOG-RDGZ-00164383 at -387).

211. In Appendix J, I have included Google's produced fields for each of the 16 logs that Google produced which contain (s)WAA bits. That appendix includes an "Ads Fields" tab that contains example field names which may fall under each of the data categories below. Note that given the preset row height in Appendix J, only a subset of the field names in each cell is visible. Since Google neither provided field descriptions nor data for these logs, should Google challenge my opinions about these fields, I reserve my right to supplement my opinion with any additional information Google may present.

212. The produced fields for the 16 logs reveal that Google collects at least the following categories of information:

- WAA/sWAA bit
- Timestamps
- App ID and content information
- IP address, User Agent
- Device information
- User Identifiers and ID linking/mapping information
- User profile and demographics information
- User geolocation and travel history information
- Analytics information
- Firebase and AdMob information
- Billing information
- User Controls
- Fingerprinting information

213. Google has been misleading in its characterization of the relationship between ads and analytics logs. In Google's Response to Request for Admission No. 18, Google stated that the "Adqueries log may include 'bits' regarding WAA status in event-level data, but the Adqueries log does not include any indicator as to whether the event relates to Google Analytics for Firebase."

However, the produced fields for the "[redacted] log contain at least the analytics fields listed below this paragraph. These analytics fields uniquely identify (1) the relevant non-Google app through the [redacted], (2) a specific installation of that app on a particular device through the GA4F "[redacted], (3) the analytics hit bundle through the [redacted]", (4) the ad event through the [redacted], and (5) other IDs. In addition, many fields record biddable Firebase app conversion tracking. These fields accordingly reveal close ties between ads and analytics data.

214. The "[redacted] (and many other logs) contains at least these analytics fields:

[redacted]

215. I will now explain the categories of information stored within the 16 logs with (s)WAA bits:

216. [redacted] (Appendix J, "Ads Fields" tab, columns D and E)

- [redacted] Google has not been forthcoming about the [redacted] contained in these 16 logs. However, Google highlighted (in green) field names containing the phrase [redacted] (see Appendix J). This phrase does not appear in Google's produced documents aside from GOOG-RDGZ-00210433, which is the produced Adevent data (I will discuss the data in this log in Section VII.B.3.b of this report and in Appendix G). Other fields that Google did not highlight include the phrase [redacted]". This phrase also does not appear in Google's produced documents aside from GOOG-RDGZ-00210433. However,

as I discussed in Appendix G, Google responded that a [redacted] field contains the sWAA bit and it is possible that fields containing [redacted] also contain the sWAA bit.

- **WAA bit**: Several other fields contain the word [redacted] As I explained earlier, [redacted] stands for [redacted] Google's internal documentation explains that [redacted] is also known as WAA (GOOG-RDGZ-00086870 "[redacted] Activity)"). Thus, field names containing the phrase [redacted]" or [redacted] may contain the WAA bit. As can be observed in Appendix J, [redacted] tab, column E, these fields only appeared in non-GAIA logs.

217. **Timestamp (**Appendix J, "Ads Fields" tab, column F) – Google keeps timestamps for every ad event and stores these timestamps in fields containing the phrase [redacted]".

218. [redacted] **(**Appendix J, "Ads Fields" tab, column G) – Google keeps its app IDs and information related to app IDs in a variety of fields containing the phrase [redacted]. From the produced data, I have observed the Google [redacted] field containing the name of the app and the Google [redacted] field containing an app identifier that indicates whether the app is on Android or iOS (*see, e.g.*, Appendices C and F).

219. **Content (**Appendix J, "Ads Fields" tab, column H) – Google keeps information about the content the user is viewing in a variety of fields. These include the initial ad request or query, content URLs, and referer URLs. The URL of the specific content includes folders and subfolders that describe what the user is viewing, including the exact screen. For example, in Appendix F, I have observed a "content_url" field in ads events recording full URLs such as:

- https://www.foxnews.com/entertainment/titanic-director-james-cameron-new-investigation-will-settle-jack-rose-door-debate
- https://fandomwire.com/can-smell-the-mcu-fans-tears-james-camerons-avatar-2-is-inches-away-from-dethroning-avengers-infinity-war-to-reach-top-5-highest-grossing-movies-ever/
- https://www.lamansiondelasideas.com/en/present/walmartend-theft-with-banana-trick-self-checkout-system/

In addition, since ad events store analytics IDs and since analytics data contain screen view and page view information, one can locate corresponding analytics events containing app screen and

page names. In addition to the content URL, the referer URL is a standard HTTP header parameter that contains the URL of the domain that led the user to a particular app screen or page.[139] I have observed referer URLs in produced data (e.g., Appendix F).

220. **IP address (**Appendix J, "Ads Fields" tab, column I) – Google keeps users' public IPv4 and IPv6 addresses in several dedicated fields. Google's internal documentation considers IP address as a fingerprinting attribute, where fingerprinting is "[a] Unique or probabilistically Unique combination of software, hardware, or network attributes for the purpose of identifying or tracking a device, app, browser, or User" (GOOG-RDGZ-00189024 at -024). Another document explains that "Fingerprinting technologies typically rely on heuristics such as IP address that identify users across various touch-points and generate a 'fingerprint ID' to identify the user across future interactions" (GOOG-RDGZ-00201612 at -668).

221. **User Agent and other device attributes** (Appendix J, "Ads Fields" tab, columns J – P) – Google keeps users' device information in a variety of parameters. These parameters store device operating system and version (e.g., Android version 12), device brand (e.g., Apple, Samsung), device model ([redacted]," user bandwidth, device height and width, device resolution height and width, battery level, battery charging, volume_normalized, and other information. Even setting aside the impressive array of data that Google stores, when combined, device information and IP address will identify a user's device with high probability.

222. **User IDs and ID linkages** (Appendix J, "Ads Fields" tab, columns Q – AC) – Google stores WAA/sWAA-off data with a variety of Google identifiers. These include identifiers such as user_id, device ID, vendor ID, PPID, [redacted] and [redacted]. Google also keeps ID

[139] *Referer*, Mdn Web Docs, https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer (Last accessed February 15, 2023).

linkage information in parameters related to [redacted], which I will discuss in Section VII.G. Notably, while only personal logs contain "gaia_id," non-personal logs have a parameter that indicates [redacted]." Google did not explain where this GAIA ID is stored for events in non-GAIA logs. On the other hand, GAIA logs contain a parameter that indicate [redacted]," Google did not explain where this device ID is stored for events in GAIA logs. In addition, GAIA logs contain a variety of encrypted non-GAIA identifiers, such as userid, vendor ID, and app_instance_id. These other identifiers also appear in non-GAIA logs. Google also stores PPID in both GAIA and non-GAIA logs. Several other fields store information related to GAIA, DSID, and ADID/IDFA. These parameters appear in both GAIA and non-GAIA logs.

223. **User Demographic and Profile** (Appendix J, "Ads Fields" tab, columns AD – AE) – Google keeps user age and gender information in both non-GAIA and GAIA logs. Additional user profile information Google keeps include user interest segments, ad click and view habits, college_student, education, home_ownership, household_income, industry, parent, parenting_stages, and relationship_status.

224. **User Geolocation and Travel** (Appendix J, "Ads Fields" tab, columns AF – AG) - Google keeps user location and location history information in a variety of parameters including city, region, longitude, latitude, commute distance, number of airports visited, and number of cities visited.

225. **Firebase and App Ads** (Appendix J, "Ads Fields" tab, columns AH – AJ) – As mentioned above, Google stores GA4F information in app ads logs, enabling one to look up corresponding analytics information using IDs for an ad event and app instance id. Google also stores numerous parameters related to Admob, including application and ad bidding information.

226. **Billing-related information** (Appendix J, "Ads Fields" tab, column AK) – Google stores detailed billing information for each event, including revenue and cost information.

227. **Privacy control information** (Appendix J, "Ads Fields" tab, column AL) – Google stores several fields recording privacy modifier information, including Narnia 2 and other information.

228. **Fingerprinting information** (Appendix J, "Ads Fields" tab, column AM) – Google stores numerous fingerprinting fields in both GAIA and non-GAIA logs, including fields containing phrases like "user_fingerprints" and "model_fingerprint".

229. While Google provided limited information for just 16 logs, Google's internal documentation suggests there are many more ads logs. The document labeled GOOG-RDGZ-00066703 at -709 discusses several different types of ads logs, including Raw logs, Joined logs, and Evenflow annotated ("EFA") logs. The document explains that Raw logs are "logs written by serving to record ad events. They are recorded individually for each type of event and since they are the original input of reporting pipeline, they contain all required information"; Joined logs are "one type of processed logs that user response events like view/click/conversion are joined with the ad queries. Thus, they carry over more complete information for user response events." EFA logs are "other type of processed logs after further annotating joined logs with F1 metadata and applying business logic for various purposes, e.g., revenue/billing calculation."

230. Internal Google documentation shows a multitude of different logs that contain app ads data, including where app analytics is integrated with Google app ads products. For example, GOOG-RDGZ-00066414 at -416 lists the following AdMob logs for Ad query, Ad click and Ad View (reproduced in the figure below). [redacted] are GAIA logs ([redacted] and the others are non-GAIA logs ([redacted]. As noted in the Figure below, app ads data in these logs have corresponding

GA4F events and the AdMob and GA4F data can be joined by join keys. Some of these logs are also listed in GOOG-RDGZ-00021548 at -548 and in GOOG-RDGZ-00066703 at -710 as [redacted]

[redacted]

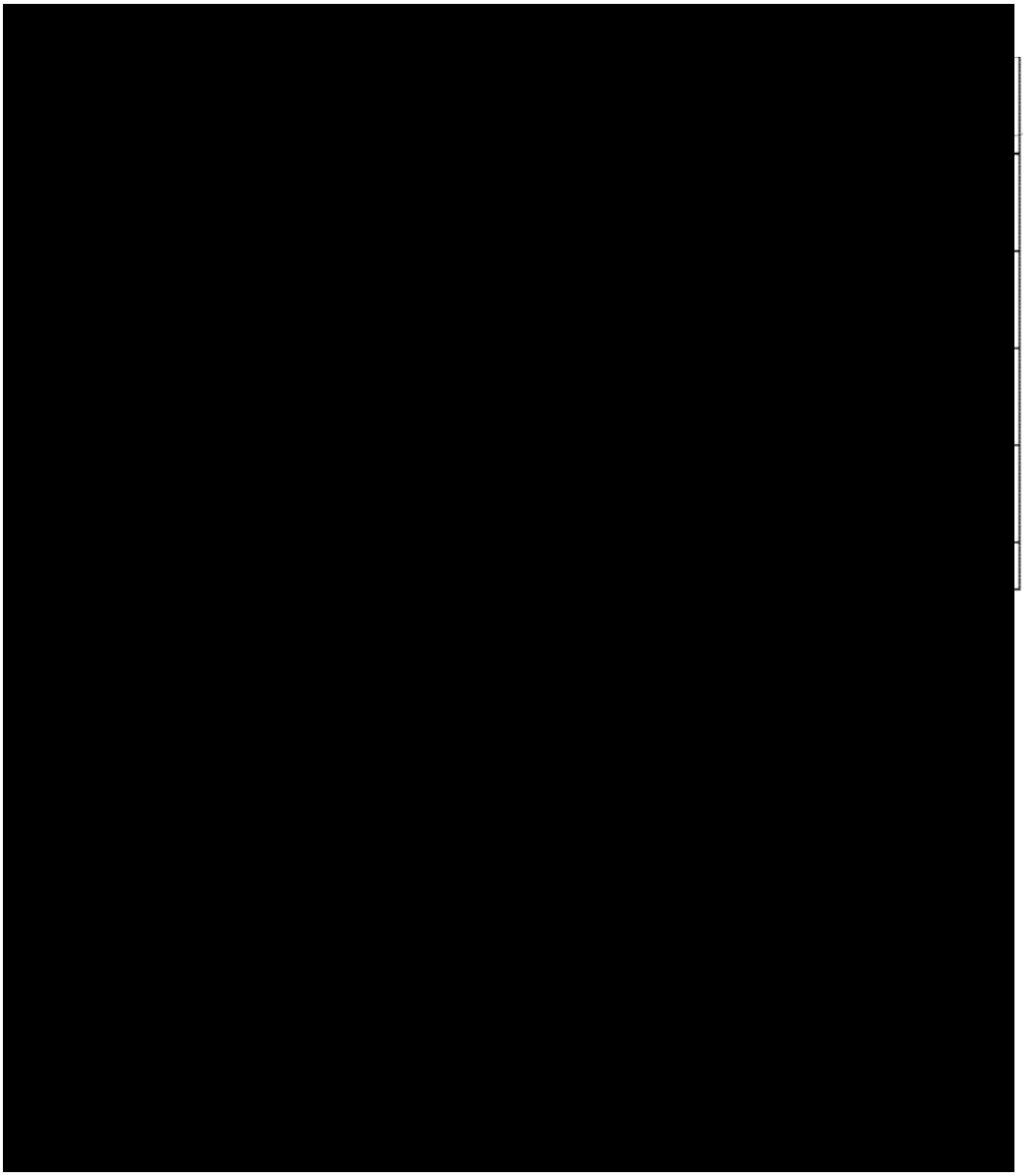
Input event	Input logtypes to import	Corresponding [redacted] event	Comments
[redacted]			

231. A set of logs from Google Ad Manager for apps are listed in GOOG-RDGZ-00060616 at -628, reproduced in the figure below:

232. GOOG-RDGZ-00027622 at -630 and -631 lists many display ads logs (both personal and non-GAIA) as well as their retention period, reproduced in the figure below. Several of these logs are retained permanently. In addition to the logs listed below, GOOG-RDGZ-00062717 at -718 identifies [redacted] as storing app conversion data. [140]

[140] [redacted] (GOOG-RDGZ-00154327 at row 26 and column G). [redacted] is a reference to display ads. [redacted] denotes Google's front-end servers.

Suggested plog source:types	Biscotti counterpart	Proto	Writer	Retention
[redacted]				



233. GOOG-RDGZ-00195736 at -740 lists several AdMob logs, including [redacted], [redacted] and [redacted] logs. GOOG-RDGZ-00130118 identifies three additional logs, including [redacted]. The latter is said to contain "All traffic where WAA is off…as well as WAA-on traffic that is not directed at a search property."

234. During Google's 30(b)(6) witness Belinda Langner's deposition, Google's counsel identified the [redacted] as a "pre-attribution log source"

and [redacted]s as a "post-attribution log source" (Langer Tr. 203:14-204:22). Ms. Langner described these logs as containing sWAA-off AdMob data (Langer Tr. 209:6-211:3). Ms. Langner also discussed "raw conversion" logs (Langer Tr. 204:15-22). On March 8, 2023, Google provided a follow-up declaration from Ms. Langner confirming that "[redacted]

235. In Google's Supplemental Response to Interrogatory No. 17, Google produced WAA opt-out rates from data stored in a [redacted] log. [redacted] The stored data dates back at least to April 18, 2016 and contains WAA-off data related to Search Ads, Display Ads, and YouTube Ads. Google did not provide any information about how this log was created, what "sampled" means, and the number of samples for each of the 25 random days that Google unilaterally selected to produce data. It is entirely possible for any of the produced percentages to be based on just a single sample (e.g., a single person whose WAA is set to "off" on that particular day). For example, [redacted] Given the percentage of Google accounts that had WAA enabled at that time, the statistics Google produced from the [redacted] log are highly unlikely to be representative of the WAA and sWAA status of Google's traffic.

236. Google subsequently produced a spreadsheet (labeled GOOG-RDGZ-00204474). Two of the tabs named "WAA Opt-out Impressions" and "WAA Opt-out Clicks" contain the same data as

that produced in Google's Supplemental Response to Interrogatory No. 17. However, Google included two additional tabs labeled "WAA Opt-out Impressions (US only)" and "WAA Opt-out Clicks (US only)," which appear to be US-only percentages. This seems to suggest that the percentages in Google's Supplemental Response to Interrogatory No. 17 are not limited to the United States (Langner Tr. 178:20-179:7).

237. On February 14, 2023, Google provided a Second Supplemental Response to Interrogatory No. 17. The US WAA opt-out rates shown in GOOG-RDGZ-00204474 were reproduced in this supplemental response. In addition, Google provided US, sWAA opt-out rates on Google's Display Advertising Stack with percentage values shown for only three days in 2022. These percentage values were, once again, drawn from the [redacted] log. But as before, Google did not provide any information about the log, how it was created, nor the contents stored within. It is unclear why there were "null" values on days other than the three days with percentage values. Furthermore, since Google's Display Advertising Stack includes both display ads from websites and from apps, it is unclear how these percentages apply to app ads.

b. Plaintiff and Test Device Ads Data Analysis

238. While there are many logs and data storage repositories that may store WAA or sWAA-off app ads data, Google limited its data production to the following:

- "[redacted]" in GOOG-RDGZ-00182689, and in the February 23, 2023 production
- [redacted] in GOOG-RDGZ-00182721, and in the February 23, 2023 production (reproduced on March 15, 2023)
- [redacted] in the February 23, 2023 production

239. The [redacted]" log and [redacted] do not appear to contain what I could discern as a WAA or sWAA bit or field. [redacted]" may contain a sWAA

bit, although the produced WAA-off data in this log appear to be from Google's O&O apps, not from non-Google apps.

240. Google did not provide any schema for what is contained in these data repositories. As with the Analytics data production, Google did not produce the search script Google engineers used to locate the data using the submitted user IDs. As a result, I cannot determine what date range was searched for and whether Google placed any filters that limited the produced results. In addition, when a search did not produce responsive data (for three of the five submitted Plaintiffs' ADIDs), Google did not provide any explanation as to why.

241. Moreover, the log [redacted]" does not appear in Google's document production for this case. Given Google's agreement that this log is relevant, I would have expected to find documents about this log in the document production.

242. Several internal Google documents and deposition testimony provide a bit of background on [redacted] is a [redacted] platform that "collects, processes and stores all user app data for app ads products" (GOOG-RDGZ-00181440 at -441). Google explains in the same document that [redacted] collects [redacted] data as well as Gaia data.[141] GOOG-RDGZ-00200228 at -248 shows [redacted] can be "[redacted]." The same document at -251, reproduced below, shows user app data stored with different IDs in Kansas. Belinda Langner testified that "The [redacted] data store, right, stores the information that we have from the GA for Firebase data … against some sort of key. And in this case, we are talking about the device ID key, let's just, for the purposes of this discussion, add IDFA or Ad ID" (Langer Tr. 90:14-20). When asked about conversion measurement data, Ms. Langner explained that it is

[141] GOOG-RDGZ-00181440 at -441: [redacted]

stored in [redacted] and keyed to device ID (Langner Tr. 145:16-147:2); however, Ms. Langner stated that "When the user has sWAA or WAA turned off, the Google Ads systems do not log the specific information on that user in -- into the [redacted] profile -- into the [redacted] data store" (Langner Tr. 89:12-16, 90:3-11, 91:6-22). As I will discuss, this statement appears to be inaccurate. Google does log users' WAA/sWAA-off data in [redacted], as Google's data production reveals.

[redacted]

243. The Device ID-based data follows a flow where "All conversion events are written to app user data [K]ansas on device ID space… [redacted] processes these events and produces serving columns in device ID and biscotti space" (GOOG-RDGZ-00181440 at -441). GA4F collects event data "with Gaia id as well as device id" (GOOG-RDGZ-00181440 at -442). Google uses the GAIA ID to "lookup user consent status" and stores WAA-off and sWAA-off data in non-GAIA logs (GOOG-RDGZ-00181440 at -442–443). The consent checks include [redacted] Unicorn users (kids users), and NPA (non-personalized ads) (GOOG-RDGZ-00181440 at -443 and -444). The document labeled GOOG-RDGZ-00182145 likewise explains at -148, [redacted] maintains user installed apps (in Gaia and Device profile) by aggregating data from 3 sources,"

including from "[redacted] and "from [redacted] for app engagement and user activity from ad requests."

244. My analysis of the data in the [redacted]" log is in **Appendices C and G** of this report. Google produced Plaintiff Anibal Rodriguez's data (corresponding to ADID: [redacted] covering dates May 18, 2022 to August 18, 2022. As shown in **Appendix A**, Anibal Rodriguez's signed-in account, [redacted] had WAA and sWAA turned off during this time. The stored data includes ADID, app_id (which shows the names of the apps he used), user_agent (which identifies the device as a Samsung Galaxy phone[142]), GA4F SDK version, conversion events (e.g., session_start, first_open, login, payment_success, etc.[143]), conversion ID, and geolocation information, among other information. Google also produced data from the four test devices corresponding to submitted device identifiers (ADID and IDFA). As discussed in Appendix G, it is readily apparent whose data each event belongs to from the device identifiers.

245. The WAA/sWAA status of each event in the [redacted]" log can be readily determined based on stored timestamps. As shown in **Appendix C**, Google intermixes WAA-on/sWAA-on, WAA-on/sWAA-off, and WAA-off/sWAA-off data within the same log, with data stored the same way regardless of these user control settings.

246. My analysis of the produced data in [redacted] is in **Appendices D and G** of this report. The produced data from Plaintiffs are included in the "GOOG-RDGZ-00182721" tab while the produced test device data is included in the "2023-02-23 Prod" tab. Plaintiff Anibal Rodriguez's

[142] *See* Appendix C "Combined Records" tab, column K containing user agent "Dalvik/2.1.0 (Linux; U; Android 12; SM-G991U Build/SP1A.210812.016)". "SM-G991U" is a Samsung Galaxy S21 phone. "Build/SP1A.210812.016" is Android version 12 compiled on 2021-08-12.
[143] *See* Appendix C "WAA sWAA Status Analysis" tab, column Q.

data (corresponding to ADID: [redacted] covering dates February 21, 2021 to July, 28, 2021, is reformatted and shown in column format in the [redacted] Data Reformatted" tab. I have also added reformatted test device data to the same tab. While [redacted] may contain a multitude of app information, Google only produced conversion-related data, including conversion events such as session_start, first_open, app_open, navigation, and others.[144] As shown in Appendix D and discussed in Appendix G, Google intermixes WAA-on/sWAA-on, WAA-on/sWAA-off, and WAA-off/sWAA-off data within the same [redacted] storage, with data stored the same way against non-GAIA identifiers regardless of these user control settings. Google also stores WAA/sWAA-on GAIA data in [redacted] with data stored in a similar fashion as non-GAIA data.

247. My analysis of the produced data in Adevents is in **Appendices F and G** of this report. This production appears to contain mostly, if not all, GAIA data from Google O&O and non-Google apps. As with non-GAIA logs, Google also intermixes WAA-on and WAA-off data within GAIA logs. Many produced WAA-off data are stored with GAIA IDs.

248. Importantly, as I discuss in Appendix G, several events contain both GAIA ID and [redacted] for non-Google app data. Other events store unencrypted ADID and [redacted] for non-Google app data. These events are also stored either with IPv4 or IPv6 addresses along with user agent and associated device information. The presence of these unencrypted and encrypted non-GAIA identifiers in GAIA logs, as well as the presence of a user's IP address and user agent in both GAIA and non-GAIA logs, can effectively link GAIA and non-GAIA data containing the same identifiers or IP address/user agent.

[144] *See* Appendix D "UUAD Data Reformatted" tab, column K for conversion event names.

C. Google Does Not Provide Users with Control Over Google's Collection and Saving of WAA-off and sWAA-Off Data.

249. It is my opinion that Google, throughout the class period, has uniformly not provided users with any control that stops Google from collecting and saving the WAA-off and sWAA-off data at issue in this case.

250. As discussed in the previous two sections, Google's consent check process (to determine WAA and sWAA status) for analytics and ads data takes place on Google servers, rather than on user devices. As such, analytics and ads data from users' activity on non-Google apps are sent to Google and saved on Google's servers regardless of users' WAA and sWAA settings. Once the consent check is complete, Google logs the data either with a user's GAIA ID (for example if WAA / sWAA is "on") or non-GAIA identifiers (when WAA /sWAA are "off").

251. There is also no way to prevent Google from saving WAA and sWAA-off data once it is logged after the consent check process is complete. Google employees have admitted that Google does not provide any way for users to prevent Google from collecting and saving their activity on non-Google apps. When asked if he is aware of *any* Google control that would stop Google from collecting any data about a user's app activity, Eric Miraglia, the Founder of Google's Privacy and Data Protection Office, responded "I'm not aware of any setting that -- that's shaped exactly the way you described it" (Miraglia Tr. 96:21-97:6, 128:21-129:3). Similarly, when asked if Google ever considered making the WAA setting "completely turn off data collection", Mr. Monsees responded that he didn't "believe that was ever considered." (Monsees Tr. 302:18-25).

D. Google Does Not Provide a Way for Users to Delete WAA-off and sWAA-off Data.

252. It is my opinion that, throughout the class period, users have had no ability to delete WAA-off data and sWAA-off data. As an internal Google document explains, "Logs contain certain events for WAA disabled users, which: … have no transparency, have no control, no ability to

delete, etc." (GOOG-RDGZ-00118124 at -125). By contrast, WAA- and sWAA-on data can be viewed by users in My Activity and deleted from Google logs and data sources to some extent.[145] Ironically, Google offers WAA- and sWAA-off users less transparency relative to WAA/sWAA-on users because the latter group are able to view their data. As summarized by software engineer Chris Ruemmler, "[s]eems sort of silly to turn [WAA] off as I'm not any safer with them off than on" (GOOG-RDGZ-00024709).

253. For data tied to a user's non-GAIA identifiers, I have found no information that users can view or delete that data using any tools offered by Google. When asked "where a person could go to review and delete pseudonymous data that was generated from their interactions with apps," the Founder of Google's Privacy and Data Protection Office (Eric Miraglia) testified that "I'm not specifically familiar with the control set that governs that data" and he could not identify any way for users to delete that data from Google's servers (Miraglia Tr. 134:14-137:19).

254. Relatedly, former employee Greg Fair admitted: "I'm not aware of a specific control that the user can delete something from Google. The controls that we have in in the My Activity space talk about deleting a piece of data from your account" (Fair Tr. 79:6-10). Rahul Oak also testified that data tied to a Device ID is far less transparent and subject to fewer privacy controls (Oak Tr. 246:18-250:11).

255. Google in this case has relied on the relationship between app developers and users to try to excuse the fact that Google offers no way for users to delete WAA-off and sWAA-off data. Steve Ganem claimed during his deposition that users do not have a way to delete this data because

[145] [redacted] (GOOG-RDGZ-00161364 at -402 and GOOG-RDGZ-00118045). Greg Fair testified that "The controls that we have in the My Activity space talk about deleting a piece of data from your account. The web and app activity setting that we were addressing here relates to saving data or storing data, saving data to your account. When that setting is off, data is not stored into the account. When you go into My Activity to delete a search, individual search or multiple searches, that is deleted from that repository that's associated with the account is my understanding" (Fair Tr. 79:8-18).

"the stream is something that belongs to the business and contains data related to all users of that app and their device. So an end user shouldn't have the ability, for security reasons, to delete the stream" (Ganem Tr. 150:22-25).[146]

256. Mr. Ganem's position cannot be squared with the position taken by Google's CEO Sundar Pichai in sworn testimony to the United States Congress. In December 2018, Mr. Pichai testified to Congress: "For Google services, you have a choice of what information is collected, and we make it transparent. […] In fact, in the last 28 days, 160 million users went to their My Account settings, where they can clearly see *what information we have*—we actually show it back to them. We give clear toggles, by category, where *they can decide whether that information is collected, stored*, or—more importantly—if they decide to stop using it, we work hard to make it possible for users to take their data with them."[147] Mr. Pichai thus assured Congress that Google provides tools for users to view and delete their data. But that is not the case for WAA- and sWAA-off data. For that data, as confirmed by the above information, there is no way for users to review that data, nor does Google provide any way for users to delete that data.

257. Since "data is the gold of the 21st century," the ability for users to delete data stored at Google "has been sacrificed on the altar of performance and scalability," with Google admitting that "Really Deleting Data is HARD" (GOOG-RDGZ-00161364 at -401). Google further admits that "It isn't always obvious where the data lives"; "Even when we know where it is, it's still hard"

[146] Steve Ganem also discussed controls that app developers *may* offer end users: "End users, they could, if the developer offered, request that their data be deleted from the analytics property. We offer our developers an API to respond to that request by deleting that user's data, whether it's the app instance ID or user ID from the analytics data." (Ganem Tr. 152:11-16). But he did not identify any examples of an app providing such a deletion option. Insofar as there are any apps that provide such an option to users, that would support my opinions that WAA- and sWAA-off data is linked to users. *See infra* Sections VII.G and I.

[147] Sarah Perez, "*Google's CEO Thinks Android Users Know How Much Their Phones Are Tracking Them*," TechCrunch, https://techcrunch.com/2018/12/11/google-ceo-sundar-pichai-thinks-android-users-know-how-much-their-phones-are-tracking-them (Last accessed March 17, 2023) (emphasis added).

and even though Google has some infrastructure for wipeout, "things still fail" (GOOG-RDGZ-00161364 at -404 to -407).

E. App Developers Have No Way to Prevent Google from Collecting or Saving WAA-off and sWAA-off Data.

258. Throughout the class period, app developers have had no way to prevent Google from collecting and saving WAA-off and sWAA-off data.

259. To be sure, app developers have options to prevent Google from collecting data associated with their respective apps. But these options are not specific to WAA-off and sWAA-off data.

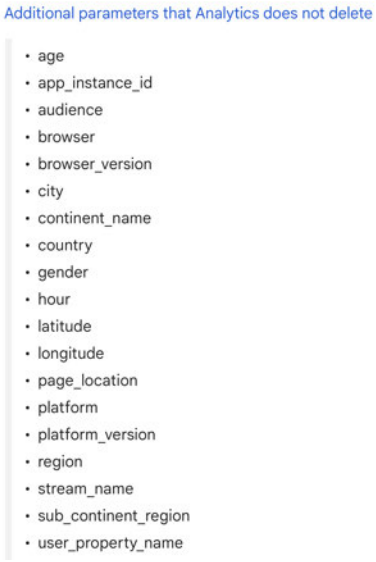
260. For example, Google provides app developers with a setting to permanently disable all GA4F data collection or temporarily disable collection.[148] However, these settings disable GA4F data collection for *all* users of the app.

261. As I discuss in Appendix I, I have not found information suggesting Google provides app developers with any setting that would disable only Google's collection or saving of data from users who have turned off WAA and/or sWAA. Nor am I aware of a developer setting that allows app developers to specifically delete WAA-off or sWAA-off data.

262. Similarly, Google provides app developers with limited mechanisms to delete analytics data. "App developers can [] delete their Google analytics account, which deletes app measurement data they have sent to Google pursuant to Google's wipeout policies (i.e., within a certain period of time after the app developer opts to delete their analytics account)" (Google's Resp. to Interrog. No. 18). But that option of course is not specific to WAA-off and sWAA-off data.

[148] *Configure Analytics Data Collection and Usage (for Android)*, Firebase https://firebase.google.com/docs/analytics/configure-data-collection?platform=android (Last accessed March 17, 2023);*Configure Analytics Data Collection and Usage (for iOS+)*, Firebase *https*://firebase.google.com/docs/analytics/configure-data-collection?platform=ios (Last accessed February 15, 2023).

263. In addition, there are some parameters that Analytics does not delete, including the ones shown in the figure below[149].



264. Google also claims that App developers may delete user data associated with non-GAIA IDs.[150] However, since Google does not inform app developers of a user's WAA/sWAA setting state, there is no mechanism for app developers to identify WAA-off or sWAA-off data for deletion.

265. In an Interrogatory response, Google claims that app developers who use GA4F "are required by Google to disclose their use of [GA4F] to their end users [often through privacy policies] and obtain their consent, where necessary. Many such developers provide their end users with a way to opt out of analytics usage, and/or to delete data the developer has collected from that user's device and sent to Google" (Google's Resp. to Interrog. No. 18; *see also* Google's Resp. to Interrog. No. 21, 12:19-23).

[149] *[GA4] Data-Deletion Requests*, Analytics Help, https://support.google.com/analytics/answer/9940393 (Last accessed March 17, 2023). Deleting an app does not delete historical data. *Delete An App*, Firebase Help, https://support.google.com/firebase/answer/7047853 (Last accessed February 15, 2023).
[150] *[GA4] User Explorer*, Analytics Help, https://support.google.com/analytics/answer/9283607 (Last accessed February 15, 2023).

266. But as discussed just above, I have not found information indicating that Google provides app developers with an option to delete WAA-off and sWAA-off Data. Nor have I found an indication that Google discloses to app developers that Google will continue to collect and save data notwithstanding whether WAA-off or sWAA are off.

267. Instead, Google represents to app developers that Google's collection of user data is governed by Google's own user-facing policies and controls. For example, the Google Analytics for Firebase Terms of Service recommends that app developers include in their own privacy policies the following Google webpage: "How Google uses data when you use our partners' sites or apps."[151] That user-facing Google webpage informs users that they can use "My Activity [] to review and control data that's created when you use Google services, including the information we collect from the sites and apps you have visited." That provision contains a hyperlink to the "My Activity" page, which is one place where WAA/sWAA can be found and switched off.

F. Google Throughout the Class Period Used and Monetized WAA-off and sWAA-off Data, Including for Purposes of Serving Ads, Tracking Conversions, and Improving Google Products.

268. It is my opinion that Google, throughout the class period, has uniformly used the WAA-off and sWAA-off data at issue in this case for its own benefit, including by monetizing it. Those uses include serving advertisements, tracking and modeling conversions, and improving Google products, processes, and services. Google has even sought to quantify the money that it makes from serving advertisements and tracking conversions, although these efforts (as far as I can tell) were not directly focused on WAA-off and sWAA-off data (e.g., GOOG-RDGZ-00188469; GOOG-RDGZ-00188768).

[151] *Google Analytics for Firebase Terms of Service,* Firebase – Support, https://firebase.google.com/terms/analytics (Last accessed March 17, 2023)

269. Based on my experience with computing systems and my knowledge of data management and the advertising business, it also is my opinion that Google's collection and saving of WAA-off and sWAA-off Data does not result in any material incremental costs to Google's business. WAA-off and sWAA-off Data constitutes a relatively small portion of traffic compared to WAA-on and sWAA-on Data. Therefore, Google's collection and saving of WAA-off and sWAA-off (or Google's lack of doing so) has no material impact on Google's planning and budgeting for infrastructure, including physical space, data warehouse capacity, personnel, and marketing.

1. Serving Advertisements While WAA or sWAA Is Turned Off

270. As discussed earlier on Section VII.A.1., on Publisher apps, ads are served through the Google Mobile Ads SDK. In Google's Answer to Plaintiff's Fourth Amended Complaint, "Google admits that AdMob is a Google product that app developers may use to monetize mobile apps with targeted, in-app advertising" (Answer ¶ 60) and "Google admits that Google AdSense and Ad Manager are products that help a user sell products on a non-Google website or app" (Answer ¶ 70).

271. Advertisements shown to users when WAA or sWAA is turned off rely on Google's collection and saving of WAA-off or sWAA-off data. Put differently, but for Google's collection of WAA-off or sWAA-off data, Google would not be able to serve advertisements to those users and then charge the advertisers because Google would lack the necessary data records to back up their advertising charges.

272. As discussed above, Google's GMA SDK sends an ad request message to Google servers when a user views a page in an app containing a slot for an ad. This process occurs regardless of whether WAA and/or sWAA are on or off (Google's Supp. Resp. to Interrog. No. 23). If WAA and sWAA controlled Google's collection of this information by way of the GMA SDK, then Google would not return the requested ad to the publisher's app. Relatedly, as explained in more

detail in the next subsection, Google could not track advertising conversions but for its collection and saving of WAA-off and sWAA-off data.

273. Google's collection of WAA/sWAA-off data also enables Google to serve targeted advertisements. In general, there are several ways to serve advertisements that are targeted. For each type of advertising campaign, ad targeting could be based on a variety of targeting signals, including the user's geolocation (determined through IP address), language, type of device, user demographics like age and gender, user interest, and the content of the website or app being viewed.

GOOG-RDGZ-00196620 at -626

274. For ad serving while a user is signed into their Google account and has switched off WAA or sWAA, Google uses data associated with ADID (on Android devices), IDFA (on iOS devices), and other non-GAIA identifiers. Even when such IDs are not available, for example if users opted out of ad tracking with Android device setting (OOOAP) and iOS device setting (LAT/ATT), data contained in ad request messages can still be used to serve ads to users (including targeted ads by way of signals such as the user's language and geolocation).

275. Google has represented to Plaintiffs that when WAA or sWAA is turned off, there is no ad personalization.[152] For example, Belinda Langner testified that "when sWAA is turned off, the Google Ads systems do not use the data collected by GA4 Analytics for Firebase for the uses of ads *personalization*" (Langner Tr. 85:15-25 (emphasis added); *see also id.* 29:5-9 (similar testimony for WAA)).

276. However, Ms. Langner does *not* claim that ads are not served when WAA or sWAA is turned off, nor that ad targeting does not occur based on non-GA4F data. To the contrary, she qualified her testimony by stating that she was "responding specifically about how Google uses the data collected from GA Analytics for Firebase" (as opposed to data collected by way of other Google code) (Langner Tr. 85:15-25). Moreover, Google's Fourth Supplemental Response to Interrogatory No. 1, Section 8—on the Use of Non-GAIA User Data by Google—explains that "Google can also use pseudonymous event data from GA for Firebase logs to target advertising to users." Relatedly, Google's Response to Interrogatory No. 15 discusses "ad targeting for anonymized ad profiles."

277. Google in this case seems to be making a distinction between "personalization" and targeting. Google defines "personalization" as "altering a user's experience based on information associated with their user id" (GOOG-RDGZ-00118124 at -24). On the other hand, Google seems to consider advertising as "targeted" but "non-personalized" when it is based on information associated with a user's non-GAIA IDs (as opposed to the GAIA Id), such as language, the type of device, and the content of the website or app being viewed. I have not found any information indicating that Google is unable to use these types of WAA-off and sWAA-off data to serve targeted advertisements.

[152] The exception may be for signed-out users (i.e., someone who is not signed into their Google account but has sWAA OFF). (Ganem Tr. 284:12-19).

278. Ad personalization is impacted by two additional user controls: GAP (GAIA Ads Personalization) and NAC (New Ads Control).[153] Because Google does not use data collected by GA4F from WAA- and sWAA-off users to serve personalized ads, such WAA- and sWAA-off data is not used for ads personalization regardless of whether GAP and NAC are turned on or off. A WAA/sWAA-off user's GAP and NAC settings influence only whether Google serves ads that are personalized based on other data sources. "[A] user with 'GAP on AND (WAA-off OR sWAA-off …)' still has appreciably greater monetization potential than a user with 'GAP off'" because a GAP-on, WAA/sWAA-off user "is eligible for a subset of personalization scenarios (such as Customer Match)" that "does not include any audience targeting based on profiles generated from persisted activity data." GOOG-RDGZ-00042152.R at -156.R. Moreover, even where WAA and sWAA are off, Google can (provided GAP is on) serve personalized ads using data collected from when the user had WAA or sWAA turned on.

2. Attribution/Conversion Tracking

279. Google also uses WAA- and sWAA-off data to track and model advertising conversions. Conversions track how users respond to prompts, including advertisements. As explained by Google employee and 30(b)(6) witness Belinda Langner: "When we talk about conversion in the context of advertising, it is . . . whether or not a specific ad led to a specific action within the app and those actions can include things such as the first open or the in-app purchase" (Langner Tr. 133:13-23). As explained by Google employee Steve Ganem during his deposition: "On the Analytics side . . . a customer can indicate which events are conversions for them. For example, a

[153] Both GAP and NAC settings are found under "Manage your Google Account" settings -> Data & Privacy -> Ads Settings. The "Ad personalization is on" slider is the GAP control and the "Also use your activity & Information…" check box is the NAC control.

purchase might be a common conversion for them. And when there is an occurrence of that event, that is marked as a conversion" (Ganem Tr, 269:20-270:2).

280. The ability to capture conversion events, as well as the ability to attribute a conversion event to a prior ad event, allows Google to demonstrate the effectiveness of its advertising platforms to the advertisers, which in turn, increases advertiser spend on Google advertising platforms.[154] But for Google's collection and saving of WAA-off or sWAA-off data, Google would not be able to attribute conversions to events (like ad clicks) that occur when WAA or sWAA is off.

281. Two attributions scenarios are relevant for this case when a user is signed into their Google account and has WAA or sWAA turned off.

- **Scenario 1**: When an ad is served through the GMA SDK (for AdMob or Ad Manager) in a 3P publisher app, Google's ability to connect this ad with a later conversion event like a purchase (on web or app) relies on Google's collection of app ads data (i.e., ad impressions, clicks, and similar data) via the GMA SDK, and the saving of this data in its logs for later attribution. If the publisher app also uses GA4F, the collected analytics data may be used as well.

- **Scenario 2**: When an ad is served elsewhere (e.g., on google.com, youtube.com, 3P websites, or a Google app), Google's ability to connect this ad with a later conversion event in a 3P app implementing GA4F relies on Google's collection of app analytics data via the GA4F SDK, and the saving of this data in its logs and data storage for later attribution.

282. Thus, Scenario 1 relies on Google's collection and saving of WAA- and sWAA-off data from publisher apps implementing the GMA SDK (and GA4F if available). Scenario 2 relies on Google's collection and saving of WAA- and sWAA-off data from advertiser apps that use GA4F. Some studies have reported a 10% - 20% performance uplift when advertising platforms are

[154] "[W]e do conversion measurement as a way to show the value that the Google app campaigns have brought to a specific advertiser" (Langner Tr. 215:11-14). This is true even when sWAA is turned off (Langner Tr. 215:15-218:4).

integrated with GA4F (GOOG-RDGZ-00196222 at -244). If Google stopped collecting and saving WAA/sWAA-off data from users' activities on non-Google apps, both attribution scenarios would fail.

283. For example, for App Campaigns,[155] also known as "App Promo," advertisements promoting apps can be run on websites and in apps, including in apps that use the GMA SDK.[156] "App campaigns can show ads across the various different Google properties and Google's ad networks. App campaigns can show an advertiser's app promotion ad within search or what we would call Google.com" (Langner Tr. 161:17-22).

284. In a particular scenario where an app ad click led to a conversion event in a different app, Ms. Langner explained the conversion attribution flow as follows: "The Google Ads systems can choose to display an ad to a specific user like we talked about within an app, okay? That user can then click on that ad. That information is all logged. When a user then is taken to the App Store, downloads the app and then opens the app for the first time, Google Analytics for Firebase may send a first open event assuming a number of the conditions that we talked about, right, including the fact that . . . Google has to do something called an attribution so we have to confirm on the ad side that this specific device, IDFA or Ad ID, was shown the ad and then the attribution happens on that specific conversion event" (Langner Tr. 156:14-157:10).

[155] "[A]pp campaigns is an ad campaign type, right, that allows advertisers to promote their app, their mobile app" (Langner Tr. 109:11-14). See Appendix E for a discussion of other types of advertising campaigns.

[156] "So AdMob, right, shows ads that allow advertisers who want to promote their app, right, and there are also advertisers that want to promote their website" (Langner Tr. 111:22-112:1) and "So app campaigns, right, are -- are campaigns where an advertiser can promote their mobile app, right, and they -- and through this, advertisers can specify the specific app conversion that they want to drive towards. These types of events can include things that I mentioned earlier such as first open and in-app purchases. Google then decides to show those advertisements promoting that advertiser's mobile app on various different properties and the Google ad -- and the Google ad networks that we -- we have, including AdMob, as we had mentioned" (Langner Tr. 118:23-119:13). Google . . . chooses to optimize to find the right users who may be more likely or have a higher propensity to perform those specific actions that the advertisers specified" (Langner Tr. 151:2-152:5).

285. Ms. Langner also testified about the role played by GA4F for conversion tracking, particularly for App Campaigns. "Google app campaigns use[] app conversions for reporting to advertisers in our app campaigns," (Langner Tr. 25:16-18) and "GA analytics for Firebase, GA4F, specifically collects app conversions and so that is specifically relevant for advertisers who are promoting their app" (Langner Tr. 112:5-9). GA4F is used to "collect data, specifically app conversion data, and that includes certainly first opens, right, so when a user first opens, or in-app purchases or other specific events that a developer would -- would define in Google Analytics for Firebase" (Langner Tr. 113:19-114:1). "[W]hen it comes to the Google Analytics for Firebase data, all of the conversions that happen within a specific app and are collected by Google Analytics . . . . App conversion data can be used then, right, by the Google Ads systems and so -- and -- and that's primarily used by app campaigns" (Langner Tr. 147:24-148:7).

286. In written discovery, Google has separately admitted that it tracks conversions for app campaigns (i.e., App Promo) by way of GA4F. [redacted]" (Google's Supp. Resp. to Interrog. No. 17). [redacted]

287. Ms. Langner also explained that Google uses non-GAIA identifiers to track conversions. "Specifically for Firebase conversions, Google uses pseudonymous identifiers, such as IDFA or ADID for the purposes of conversion measurement" (Langner Tr. 32:10-13). "For Google Analytics for Firebase data, when the user has sWAA-off, the Google Ads systems can use data in this pseudonymous space for the purposes of conversion measurement" (Langner Tr. 185:13-17). Mr. Ganem, another 30(b)(6) witness, provided similar testimony. In response to a question about whether Google uses IDFA and ADID for conversion tracking, Steve Ganem responded, "Yes, it

does" (Ganem Tr. 251:13). Mr. Ganem continued: "Yes, for example, when a user clicks on an ad, say, from another ad network, and the IDFA and ADID are collected, and they eventually convert. . . . [A]ssuming that the IDs are available, then Google Analytics will do a match between them and match the conversion to the click" (Ganem Tr. 251:20-25, 252:5-8) (describing how, if "ADID and IDFA are available, [Google] would do a Device ID-based conversion measurement")).

288. Ms. Langner also described how Google ultimately benefits from its ability to track conversions. "In the context of ads, advertisers are able to target for users who are more likely to do a specific event … and Google makes money by driving more -- through the ad impressions and the ad clicks that we drive to -- to help app advertisers reach their marketing goals" (Langner Tr. 213:15-23). "The app campaigns will try to find more users that are likely to perform those actions, and advertisers specify specific target that they would like to pay for every single action and Google tries to optimize towards those targets. So by driving -- by basically, you know, advertisers, when we reach their goals, you know, may -- and reach their ROI goals may -- may choose to adjust their budgets accordingly with -- with Google and the Google Ads systems" (Langner Tr. 214:10-215:1).

289. Steven Ganem provided similar testimony. "in the event proto, there's - sort of the event proto tab, there's an indication, for example, of the event name. And if that was an event that the customer had marked as a conversion, then there would be an – basically, we would know that that is an event that the customer deems important" (Ganem Tr. 270:15-20).

290. Google's trillion-dollar advertising engine relies on ad performance measurements that report to advertisers how effective their ads have been and prove that Google's ads meet industry standards for traffic quality.

291. In its response to Request for Admission No. 37, Google denied using WAA-off data to track, model, or measure conversions that occur across Google and non-Google properties, but other discovery contradicts that assertion. For example, in Response to Interrogatory No. 15, which asked about "how Google currently uses and previously . . . has used WAA-off Data," Google admitted that Google uses WAA- and sWAA-off data for "pseudonymous conversion tracking." Google's Supplemental Response to Interrogatory No. 15 further explains: "DeviceID-keyed advertising interactions with an advertiser, such as views and clicks of that advertiser's ads, are joined to conversions recorded in that advertiser's app using Firebase (or other third party conversion tracking products or services)." Google tracks "when the same device that interacted with [an advertiser's] ad subsequently converted (e.g., opened their app, or made an in-app purchase, depending on how the advertiser has defined a conversion for the ad campaign)."

292. That interrogatory response cannot be reconciled with Google's response to Request for Admission No. 37, where Google denied that it "has used WAA-Off Data to track, model, or measure conversions that occur across Google and non-Google properties." If Google attributes a WAA/sWAA-off user's interaction with an advertisement in one place to the user subsequently opening that advertiser's app and/or making a purchase, then Google tracks, models, or measures conversions that occur across Google and non-Google properties.

293. Google employee Belinda Langner discussed how device-level controls available to users (i.e., LAT ATT, and OOOAP, which I discussed in Section VII.A.1) affect how Google tracks conversions.

294. But any impact to Google's ability to track and model conversions is offset by several mitigating measures. For IDFA specifically, an internal Google document explains that data generated by LAT-disabled users are "used to model conversions for LAT-enabled users" (GOOG-

RDGZ-00197928 at -930). "Modeling" is what it sounds like. For example, Google "[u]se[s] linked data as truth set to model conversions that we think are driven by a Google Ad interaction . . . . We don't associate a click with a conversion; we only guess which set of conversions are driven by our ads" (GOOG-RDGZ-00056108 at -116).

295. Google also implemented conversion modeling for iOS14.5, "serving on all zero IDFA traffic across all stacks" (GOOG-RDGZ-00197101 at -106). Google explains that "conversions whose ads originate on ATT impacted traffic will experience modeling" (GOOG-RDGZ-00142709 at -710). One such conversion modeling algorithm is a machine learning algorithm called iDog for iOS; the "beta launched in early July 2018" (GOOG-RDGZ-00193001 at -005). Other conversion modeling projects are discussed in Appendix E. Appendix E also discusses Google's implementation of an aggregated ID called GBRAID ID (Google Broad Ad ID[157]), which Google used in response to ATT for aggregate conversion tracking.

296. Moreover, advertisers can opt out of running ads campaigns against "LAT-enabled inventory" (GOOG-RDGZ-00197928 at -931). As for Android, the loss of ADID is "limited to loss of measurability for view-through based conversions (EVCs and VTCs), as well as losses due to undetected IVT [invalid traffic[158]] traffic" (GOOG-RDGZ-00208099 at -105). Contextual Advertising and frequency capping (limiting the number of times an advertisement is shown to the same user) are not impacted by ADID (GOOG-RDGZ-00208099 at -103).

3. Improving Google Products, Processes and Services

297. Aside from using WAA-off and sWAA-off data for serving advertisements and tracking conversions, Google also used WAA-off and sWAA-off data for product development, improvement, and diagnostics. Google's 4th Supplemental Response to Interrogatory No. 1,

[157] GOOG-RDGZ-00178406 at -407
[158] GOOG-RDGZ-00189134 at -139

Section 8 explains: "Google uses user data collected via GA for Firebase across teams for product development, improvement, and diagnostics." Google's 4th Supplemental Response to Interrogatory No. 1, Section 7 likewise explains that "GA for Firebase allows sharing Analytics data with Google for improving Google products and services, enabling technical support, benchmarking, and sharing with Account Specialists." Google's Response to Interrogatory No. 18 similarly states: "Mr. Eric Miraglia testified that when WAA is off, data is "logged for product improvement purposes" (Miraglia Tr. 210:1-5). As far as I know, Google has not in this case provided a list of products and services that were developed with and/or rely on WAA-off and sWAA-off data.

298. I can infer that Google may have used WAA-off or sWAA-off data to improve particular Google products and services.

299. [redacted] GOOG-RDGZ-00208099 at -104 explains that [redacted] (*id.*). [redacted] [redacted] (*id.*).

300. [redacted] The document labeled GOOG-RDGZ-00188409 describes [redacted]

[redacted] (*see* Appendices G, H.1 and H.2). [redacted]

G. WAA-off and sWAA-off Data is Linked to Users.

301. It is my opinion that, throughout the class period, Google's trove of WAA-off and sWAA-off data is linked to users.

302. Google has claimed that the data at issue in this case is "pseudonymous." Google tellingly chose that word rather than "anonymous." As explained by the Founder of Google's Privacy and Data Protection Office, Eric Miraglia, "we would use 'anonymous' to refer to data that cannot be tied to a data subject whereas pseudonymous data, in some cases, may be." "Pseudonymity is usually … referring to data that has not been mathematically anonymized. And so there's always at least the hypothetical possibility of reidentification" (Miraglia Tr. 106:16-107:13). The implication of Mr. Miraglia's testimony is that the so-called "pseudonymous" data at issue can be joined to users, though I think he is soft selling the risk of "pseudonymous" data being re-identified.

303. Internal documents are consistent with Mr. Miraglia's testimony, revealing that Google employees acknowledge that so-called pseudonymous data is linked to users. A Google engineer who works on GA4F has specifically flagged "joinability risks" with WAA-off data: "Some of the examples of this [sic] joinability risks" include "the ability to link app events collected by GA4F to GAIA ID even if end users turn off WAA," which "[b]reak[s] user expectations," as well as a "Subpoena: Having to retrieve Android AdId data, app_instance_id data given a GAIA ID for

users turning off WAA" (GOOG-RDGZ-00033245 at -245). Another employee followed up to clarify that "this is really expanding the ability [to join], not creating it" (*id.*).

304. I agree with these Google employees. As discussed in earlier sections of this report, Google saves a multitude of identifiers and fingerprinting information in non-GAIA logs when WAA or sWAA is turned off. I explain below how such identifiers and fingerprinting information identify users.

DSID and GAIA ID

305. As I discussed in Section VII.B, Google collects and saves users' WAA-off and sWAA-off non-Google app data from Android devices with an encrypted GAIA ID called DSID and with ADID. Google collects and saves WAA-off and sWAA-off data from iOS devices with IDFA and stores a linking table between users' IDFAs and GAIA IDs. The fact that Google can perform consent checks for class members' WAA-off and sWAA-off data on the server side means that Google necessarily links such data to class members' Google account identities and account settings.

306. On Android devices, even if Google does not collect Google Signals through GA4F for some apps on the device, as long as it collects Google Signals for at least one app on the device, the DSID sent to Google by way of the app that does collect Google Signals will identify all events from the device with other common identifiers (e.g., ADID) as coming from a particular Google account holder.

307. On iOS devices, IDFA is used to identify users. As discussed earlier, IDFA is mapped to GAIA and such mapping is stored in [redacted] (GOOG-RDGZ-00047495 at -500). The document labeled GOOG-RDGZ-00181141 at -141 explains that [redacted] sits on the boundary between unauthenticated identity and signed-in spaces" (GOOG-RDGZ-00181141 at -

141). While Google may take certain policy measures with respect to access to [redacted] data, the service itself nonetheless enables joining between non-GAIA IDs and a GAIA ID. The same document (at -143) further explains that "UDS is implemented by storing the signed-in state in server-side storage keyed by device identifiers in mobilefe [K]ansas (for IDFA and ADID) and Oz dbl (for Browser Biscotti), to enable online serving or event time lookup, represented by the UserSession proto". In addition, Google stores "offline snapshots of the [redacted]", including "IDFA-mapped Biscotti to Gaia", and "IDFA-mapped idfa to gaia) (GOOG-RDGZ-00181141 at -145).

308. Moreover, app ads traffic contains both DSID and Biscotti (IDE[159]) cookies. This Biscotti cookie is linked with other Biscotti cookies from the same user, including mobile Biscottis mapped from ADID and IDFA, as I discuss below.

309. Google has confirmed in written discovery that it uses IDFA, AdID, and DSID to track conversions, including when WAA and sWAA are turned off. Following the deposition of Belinda Langner, Plaintiffs asked Google a follow-up question: "What IDs are used for conversion measurement and attribution for users signed in to a Google account when WAA or sWAA are off?" Google's counsel replied: "IDFA, AdID, and DSID" (Jan. 30, 2023 email response). On March 8, 2023, Google provided a declaration from Belinda Langner confirming: "For Firebase ad conversions, Google uses pseudonymous identifiers (DSID, ADID, and/or IDFA) for purposes of conversion measurement. Those identifiers are described in Google's response to Interrogatory No. 1."

310. While Langner characterizes DSID as a pseudonymous identifier, Google's Fourth Supplemental Response to Interrogatory No. 1 explains that DSID "is an encrypted GAIA

[159] GOOG-RDGZ-00206388 at -399 "the [redacted]

identifier" (at page 24). Thus, even when WAA and sWAA are turned off, Google associates ads and conversion events not only through non-GAIA identifiers (like IDFA and ADID) but also through DSID, which contains encrypted GAIA ID. Google in effect associates WAA-off and sWAA-off data with GAIA, facilitating Google's tracking of conversions across multiple devices. In other words, Google uses GAIA to track conversions for WAA-off and sWAA-off users.

Device and app instance IDs

311. Although Google refers to advertising IDs (ADID and IDFA – See Section VII.A.1) as "pseudonymous" IDs, these IDs uniquely identify a user's device and all associated non-Google app data, including WAA-off and sWAA-off data. The EFF (Electronic Frontier Foundation[160] supports my opinion:

> The ad identifier is a string of letters and numbers that uniquely identifies your phone, tablet, or other smart device. It exists for one purpose: to help companies track you. Third-party trackers collect data via the apps on your device. The ad ID lets them link data from different sources to one identity you. In addition, since every app and tracker sees the same ID, it lets data brokers compare notes about you. Broker A can buy data from broker B, then use the ad identifier to link those two datasets together. Simply, the ad ID is the key that enables a whole range of privacy harms: invasive 3rd-party profiling by Facebook and Google, pseudoscientific psychographic targeting by political consultants like Cambridge Analytica, and location tracking by the U.S. military. Sometimes, participants in the data pipeline will argue that the ad ID is anonymous or pseudo-anonymous, not "personally identifying" information, and imply that it does not pose a serious privacy threat. This is not true in practice. First, the ad ID is commonly used to help collect data that is obviously personally identifiable, like granular location data. If you can see where a person works, sleeps, studies, socializes, worships, and seeks medical care, you don't need their email address to help identify them. And second, an entire industry exists to help trackers link ad IDs to more directly identifying information, like email addresses and phone numbers. In a vacuum, the ad ID may be anonymous, but in the context of the tracking industry, it is a ubiquitous and effective identifier… removing your ad ID won't stop all tracking.[161]

[160] "The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world." *About EFF*, Electronic Frontier Foundation, https://www.eff.org/about (Last accessed February 15, 2023).

[161] *How to Disable AD ID Tracking on iOS and Android, and Why You Should Do It Now*, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now (Last accessed February 15, 2023).

312. Google's internal documentation acknowledges that ADID and IDFA identify users. These identifiers (like GAIA) cannot be "blocked from joining PII" (GOOG-RDGZ-00210316 at -341).

313. As I have shown in Appendices G and H.2, if a user has sWAA turned on for a period of time before turning WAA or sWAA off, the double logged data in GAIA and non-GAIA logs link WAA- and sWAA-off data to the user's GAIA ID.

314. When ADID and IDFA are not available, I have discussed earlier how IDFV and SSAID may be collected. These identifiers identify a user's device, just like ADID and IDFA.

315. Other non-GAIA identifiers such as GA4F app instance id and Firebase instance ID (FID) identify a unique instance of an app install on a particular device. These identifiers are also unique to each device, and therefore equally identify a user's device, just like ADID and IDFA. Furthermore, app instance id can be used to link IDFV to the previously collected IDFA, since turning IDFA tracking off does not change an app's app instance id.

316. As discussed in Section VII.B.2, Google has produced GA4F data with ADID, IDFA, and app instance id, including when a user has WAA or sWAA turned off. These IDs appear in the

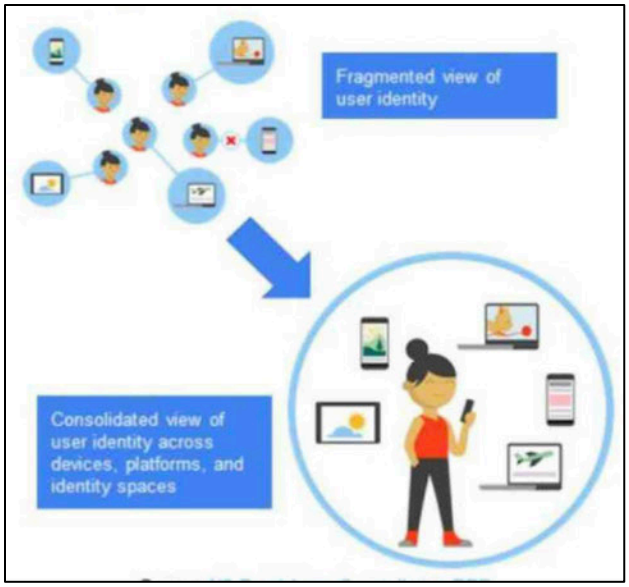
produced Analytics Baseview and ads data unencrypted. The ADID and IDFA also appear in the produced collection Analytics data unencrypted, while the app instance id appears within a "hashedAppInstanceId" field. Google has the hash function that can map any app instance id from a user's device to the stored "hashedAppInstanceId".

317. The produced data shows unequivocally that a user's WAA-off and sWAA-off data can be located using these non-GAIA identifiers. *See* Appendix G.

ID Mapping and Linking

318. Google also creates a variety of other ID linkages to form a "Consolidated view of user identify across devices, platforms, and identity space," as shown in the Figure below this paragraph (GOOG-RDGZ-00136298 at -332). This includes IDFA/ADID to Biscotti (through a project called [redacted], IDFA/ADID to Webview biscottis (through a project called Orion's belt), IDFA to Zwieback (through a project called [redacted]), and other device ID linkages through projects called [redacted](GOOG-RDGZ-00056108 at -115, GOOG-RDGZ-00029866 and GOOG-RDGZ-00136298 at -332). Google is incentivized to maintain these ID linkages for advertisement and conversion tracking purposes.[162]

[162] "All attribution is done either using device IDs (IDFA/ADID) or x-cookie graphs (e.g. [redacted]" (GOOG-RDGZ-00029740 at -742).



319. Through these ID linkages and graphs, a constellation of IDs associated with a user can be located given an ID. Below, I provide what limited information can be gathered about these linkage services from Google's document production.

[redacted]

320. When a user visits a non-Google website with Google Ad Manger or AdSense tracking, Google uses a web Biscotti ID stored in browser cookies (a small piece of text containing the ID along with timestamp and other information) to track the user as the user browses different websites. Linking this web Biscotti ID with the device ID collected from user activities in non-Google apps helps identify a user's web and app traffic as coming from the same device. As explained in GOOG-RDGZ-00206388 at -399, "The AdMob SDK (software development kit) has access to the IDFA/AdID and sends it with every ads request. One of the first steps performed by the display ads system is to map the IDFA/AdID to a Biscotti ID (called an mBiscotti when it is important to differentiate from the Biscotti ID stored in browser cookies)." The Mobius project then connects these mBiscottis to Biscottis from web browsers, which "creates a link between

admob and a website" (GOOG-RDGZ-00193938 at -949).[163] By creating such a link, ad clicks from AdMob can be linked with web activity and vice versa.[164] "There are a number of App Conversions solutions which utilize data sources such as the [redacted] app-to-web linking graph to improve Ads last click conversion coverage" (GOOG-RDGZ-00054819 at -826). [redacted] links are also used for advertising: "With increased [redacted] coverage, we can now pull web profile data for 50% of our app user queries" (GOOG-RDGZ-00166035 at -152).

321. A related project is called [redacted], which links IDFA/ADID to Webview biscottis (GOOG-RDGZ-00056108 at -115). Webview Biscottis are Biscotti IDs associated with Google's advertisement products within a Webview environment.

[redacted]

322. Google's [redacted] t "[a]nonymously bridge[s] different devices to the same GAIA ID without explicit association with GAIA (cross-device)" (GOOG-RDGZ-00136298 at -332) and "sends pings from Android devices every 24 hours or so indicating what the mapping is between Gaia and Adid. Gaia is then dropped, and the mapping is never stored" (GOOG-RDGZ-00183074 at -206).

[redacted]

323. Google also maintains "a graph of a user's Biscotti IDs" that are associated with "each device, browser and mobile app" through what is internally called [redacted] n (GOOG-RDGZ-00188195 at -199). [redacted] "uses data from two technologies": [redacted], where

[163] GOOG-RDGZ-00136298 at -332 ("Mobius - Bridge Biscotti ID and mobile browser cookie on a single device (cross-platform)").

[164] "mGDN had [redacted] – click an ad from AdMob in an app to go to web – create map between mWebBiscotti and mAppBiscotti and use for mGDN clicks" (GOOG-RDGZ-00183074 at -443). "User clicks a search ad on the mobile web, we log in the web cookie space. User lands in a mobile app and converts. Firebase or 3rd party AAP sends us a conversion event with the device ID. We join the device ID with the web cookie using [redacted] graph (GOOG-RDGZ-00202281 at -329).

"[redacted] identifies users across devices – relies on users signing in to Google services" and [redacted] identifies users across mobile apps – relies on users clicking CTW [click to website] ads from apps" (GOOG-RDGZ-00188195 at -199).[165] [redacted] "is designed from the ground to support both same device links and x-device links" (GOOG-RDGZ-00184488 at -602). [redacted], which is Google's cross-network multi-channel attribution solution, "needs to process and extrapolate across web and app impressions, clicks, and conversions accounting for [redacted] cross-device and same-device graph data (including [redacted]s and [redacted] graph data)" (GOOG-RDGZ-00192242 at -242 and -246). Google's internal documentation further explains that "[redacted] is allowed and used to connect ID spaces for at least these cases" (GOOG-RDGZ-00147439 at -454-455):

- Lookup of GAIA-id from IDFA on iOS.
- Lookup of GAIA-id from Biscotti for 3rd party exchanges.
- Propagation of {opt-out, frequency capping, mutes} from GAIA to all devices for users who switch from signed-in to signed-out.

[redacted]

324. [redacted] is a "Project name for iOS conversion tracking tying Zweiback Cookies from web to IDFA" which launched in 2018 (GOOG-RDGZ-00193001 at -006). Thus, [redacted] is like [redacted]. Whereas [redacted] links device IDs to Biscotti, [redacted] links device IDs to Zwieback IDs, which is an ID embedded in cookies associated with Google search (GOOG-RDGZ-00056108 at -115; GOOG-RDGZ-00029866 at -866). The links created by [redacted] are used at least for conversion modeling. Google explains that "With [redacted] we model conversions based on [redacted]"

[165] *See also* GOOG-RDGZ-00136298 at -332 ("[redacted] GOOG-RDGZ-00177115 at -120 [redacted]"

(GOOG-RDGZ-00200800 at -956) and [redacted] uses the [redacted] truth set to determine which conversions are likely driven by G.com clicks" (GOOG-RDGZ-00056108 at -116).

3P Signed-in IDs

325. WAA-off and sWAA-off users are identified through signed-in IDs associated with their accounts on non-Google properties. These IDs are associated with a given user's account with a specific app. For example, if I sign up for the Washington Post app, I am assigned a User-ID that is associated with my Washington Post account. These identifiers are particularly relevant to this case because non-Google apps often require users to login to the app to access the content.

326. 3P sign-in IDs such as User ID (from GA4F) and PPID (from GMA SDK) are unique IDs for specific app properties. These IDs are just as identifying as GAIA IDs since these IDs identify event-level traffic as belonging to a particular user and can be used to locate other user identifiers. For example, in Appendix B.3, a "userid" field (in "2023-02-23 Baseview" tab, Column DH) containing the value "bcbcbabb-359a-453d-a249-086babbdb3a9" was collected from activity on the Globo app on two test devices (Android 1 and iPhone 1) when WAA or sWAA were turned off. The same User ID was also collected and saved in Baseview when WAA and sWAA were turned on. This User ID was also stored in the "[redacted] log (Appendices H.1 and H.2) under a "userAttributes" field.

327. 3P sign-in IDs can also be used to locate other IDs belonging to the same user. If a user had signed into their 3P app account on different devices throughout the class period, IDs from previously owned devices may be obtained from Google logs (provided Google has not already deleted the data). As Google's internal documentation explains: "Through data already being sent or available to GA, we can potentially identify the following other IDs for that user_id, including: Biscotti IDs (one user_id may correspond to multiple Biscotti IDs; for display ads; destination:

ULS-B); Device_ids (same, could be multiple; for device ID remarketing, targeting O&O properties; destination: ULS-D); Zwieback IDs (for web RLSA[166]; destination: ULS-Z) and Firebase instance ids, for firebase registry" (GOOG-RDGZ-00203285 at -285).

Joinability with GAIA ID

328. There are multiple ways in which user's WAA- and sWAA-off data in Google logs is linked to the user's GAIA ID.

329. On iOS devices, to check the user's WAA/sWAA status, Google stores IDFA and GAIA mappings (as I have discussed in Section VII.B.2). Thus, given a user's IDFA, Google can locate the user's GAIA ID. All WAA-off data associated with the IDFA is then linked to the user.

330. On Android devices, all WAA-off data associated with the ADID is linked to the user via the Android ID[167], which is unique to each Android device. From transmissions sent from test device Android 1, I have observed both ADID and Android ID in the same transmission going to Google Play (See figure below). As shown in the figure, [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[166] RLSA stands for "Remarketing Lists for Search Ads" (Stone Tr. 171:11-15).

[167] GOOG-RDGZ-00115759 at -759 explains: "Android ID: A unique identifier supplied to an Android Device by Checkin"; "Android Checkin: A system that provides and devices with a unique identifier (Android ID) and a security token (password) that can authenticate the device".

This Android ID is hexadecimal encoded and is decoded to its decimal form as 4514249733518502807.[168] This is the same value that appears in Google Takeout (Android Device Configuration file for signed-in GAIA ID: phoenixfire202205@gmail.com) along with the device's Serial Number and other identifiers as shown below (See Exhibit B-3, Device-4514249733518502807.html file).

331. Some of the identifiers stored in non-GAIA logs are also present in GAIA logs, which enable identifiers to be joined with a user's GAIA ID. For example, Google indicates in an internal document that the "app_instance_id" is present in GAIA logs (GOOG-RDGZ-00066703 at -712). Google also explains in its Fourth Supplemental Response to Interrogatory No. 1, Section 6 that "For a set period of time, some IDs (device ID, app instance ID, and ad event ID) are stored and encrypted to allow Google to account for possible delays in data transmission and to fix any errors in data processing, including at customers' (i.e., app developers') request. Device ID and app-instance ID are stored in encrypted form for 60 days." Google does not make clear in its response where these IDs are stored in encrypted form. As discussed in Section VII.B, certainly in non-GAIA logs, I have observed device ID and app instance id in unencrypted form. Furthermore, as explained in Appendix G and shown in Appendix F, I have observed "encrypted_app_instance_id"

[168] Decoding can be done, for example, by https://www.rapidtables.com/convert/number/hex-to-decimal.html.

stored with GAIA ID in the produced Adevents data. Merely decrypting these IDs would join them to a user's GAIA ID.

332. Google also admits in its Fourth Supplemental Response to Interrogatory No. 1, Section 6, on Google's Encryption Technology, that "the ad event ID [i.e., aeid] is the only unique ID common to both GAIA space and signed-out space that would allow for joining of data to a specific user. This means that for the 6-day window in which the ad event ID is stored with encryption, it is theoretically possible for someone with access to both ad event ID encryption keys to join data." While access to the encryption keys is controlled,[169] these keys are nonetheless available, and can be used to join non-GAIA and GAIA data. Once that data is joined (within the 6-day window), the non-GAIA identifiers in the non-GAIA logs allow all previously stored non-GAIA data to be associated with a user's GAIA ID. I have likewise observed aeid stored with a multitude of other user data, which is double-logged in both GAIA and non-GAIA logs (Fourth Supplemental Response to Interrogatory No. 1). These other data can be matched along with aeid to join non-GAIA and GAIA data. Furthermore, since Google stores time-stamped events in a continuous stream as users browse non-Google apps, with event details being the same across GAIA and non-GAIA logs, data from these logs can be matched to join non-GAIA identifiers with a user's GAIA ID. Even if a user has WAA and sWAA turned off, a prior or later ID association when WAA or sWAA is on could identify the user.

Other identifying information in Google logs

333. As discussed in Section VII.B.2, I have observed users' first name, last name, email address, phone number, and zip code in Google's non-GAIA logs. Such data identifies a user.

[169] Several groups within Google may be given special access. *See* Fourth Supplemental Response to Interrogatory No. 1, Section 10 ("For each GA for Firebase pipeline system component, the current oncalls (dev oncalls and SRE) have access to the production data storage. Additionally, break-glass access using access on demand can be obtained by off-call pipeline engineers to debug production issues. This access is granted for 20 hours.").

Other traffic that does not contain this information but is tied to the same identifiers as the events containing this information, likewise identifies a user.

334. Moreover, aside from the multitude of IDs stored in Google logs which identify users, Google also stores an impressive amount of app usage information, which is itself identifying because there is effectively zero probability of two different people using exactly the same apps across the class period at exactly the same times. Furthermore, app data is associated with device location and/or location inferred from IP address (GOOG-RDGZ-00153380 at -382), which form a space-time map of a user's Internet activities. Such detailed records can uniquely identify a user.

335. For location tracking, just like for WAA and sWAA, "off" does not mean "off" for Google. Rather, "off means coarse" (GOOG-RDGZ-00153380). Instead of not saving location information for a user who disables location tracking, Google asks: "if a user disables their device location, at what level of coarseness should we infer their current location?" (GOOG-RDGZ-00153380 at -381). Google ultimately determined that "a minimum of 1 km^2 and 1000 people" is sufficient for individual events (GOOG-RDGZ-00153380 at -383). As discussed in Section VII.B.2, Google's produced data include geolocation information even for WAA- and sWAA-off traffic. Given peoples' unique movement patterns, even coarsened location data collected over time is identifying.

H. California: Google Designed its Systems to Provide its California-Based Employees with Access to WAA-off and sWAA-off Data Collected Nationwide, and Google Employees Routinely Access that Information in California.

336. It is my opinion that Google designed its systems to provide its California-based employees with access to WAA/sWAA-off Data collected nationwide, and Google employees routinely access that information in California.

337. Google maintains user data in distributed data centers and has office locations around the world. In California, Google has office locations in Irvine, Los Angeles, Mountainview, Playa Vista, Redwood City, San Bruno, San Diego, San Francisco, and Sunnyvale.[170] Of Google's over 150,000 worldwide employees,[171] about 30% work in Silicon Valley.[172]

338. Belinda Langner, who is a "product lead for app campaigns," as well as her team that "develops the features … that are available for advertisers and app campaigns," are primarily based in California (Langner Tr. 25:5-8 and 27:13-28:14). She further testified that GA4F data used for conversion tracking are primarily used by app campaigns, which means that GA4F data is used by Ms. Langner and her California-based team: "when it comes to the Google Analytics for Firebase data, all of the conversions that happen within a specific app and are collected by Google Analytics for Firebase data would need to happen within an app. App conversion data can be used then … by the Google Ads systems … and that's primarily used by app campaigns" (Langner Tr. 147:24-148:7).

339. Steve Ganem, who is a "group product manager on Google Analytics" (Ganem Tr. 16:2-3) also primarily works in California, out of the Irvine office (Ganem Tr. 13:25-14:17). GA4F falls under Steve Ganem's purview (Ganem Tr. 18:8-15).

340. Edward Weng, who was a Product Manager for AdMob until January 2021 was based out of Sunnyvale, California (Weng Tr. 10:2-3 and 15:12-17:6).

---

[170] *Our Offices,* About Google, https://about.google/locations/?region=north-america&office=mountain-view (Last accessed February 15, 2023).
[171] *Number of Full-Time Alphabet Employees from 2007 to 2022*, Statista, https://www.statista.com/statistics/273744/number-of-full-time-google-employees/ (Last accessed February 15, 2023).
[172] *Google Told its Bay Area Employees They'll Need to Return to the Office by April 4,* Silicon Valley Business Journal, https://www.bizjournals.com/sanjose/news/2022/03/02/google-plans-return-to-bay-area-offices-on-april-4.html (Last accessed February 15, 2023).

341. Rahul Oak, a former Product Manager in App Ads, was based in California and also "knew a few engineers who worked on App Ads who were based in California." (Oak Tr. 41:18-23, 278:1-8).

342. In his deposition, Dan Stone testified that he worked in California on Google Signals (as part of his overall role at Google Analytics) from the physical office, including an office located at 345 Spear Street, which had several floors with many desks on each floor (Stone Tr. 221:12-15)). Mr. Stone held in-person meetings with engineers in this office. (Stone Tr. 214:11-20). Stone also stated that he was physically present in California when accessing dashboards (Stone Tr. 219:15-20).

I. Class Member Identification: Google Has Collected and Saved WAA-off and sWAA-off Data in Ways that Identify Class Members, Though Google Also Withheld and Destroyed Data Relevant to that Identification.

343. It is my opinion that Google has, throughout the class period, uniformly collected and saved WAA-off and sWAA-off data in ways that identify class members. That said, Google has withheld and destroyed data relevant to that identification.

344. Google maintains a database which reliably shows which Google account holders turned off WAA and sWAA during the class period, and when those users did so. Users in the United States who are potential class members are those who have at least one active Google account (that has not been deleted) during the class period. Google can locate in their records users' WAA and sWAA on/off states associated with each Google account's GAIA ID, along with the date of any change to those statuses within the class period (*See* Section VII.B.1). Google admitted in its response to Request for Admission No. 36 that it has "maintained at least one dashboard, log, or table that reliably tracks WAA and sWAA on-and-off events for all Google Account Ids on an individual level.'"

345. Google can also locate in its records users' devices associated with each Google account, which means that Google knows which of its account holders have used a mobile device during the class period (*See* Section VII.B.1). Therefore, if a user had WAA or sWAA turned off at any point during the class period and the user used a mobile device, Google can notify the user by emailing that user (using the e-mail associated with the Google account) that they are a potential class member.

346. Class members can also self-identify, and Google can use its records discussed just above to verify that class members had WAA-off or sWAA-off and used a mobile device.

347. Google has also produced records showing the number of US Google accounts with WAA and/or sWAA enabled monthly from May 1, 2016 to October 1, 2022 in GOOG-RDGZ-00204475. The numbers contained excluded Enterprise (Dasher) accounts, Google employee accounts (Googlers), Supervised accounts (e.g., child accounts) and deleted accounts.

348. [redacted]

349. Class members can also attest to whether they accessed non-Google apps during the time they had WAA or sWAA turned off, and Google's records can be used to verify those claims. As discussed in Section VII.B.1, users can provide a list of apps they have installed on Android

devices by downloading their Google Play Store data from Google Takeout for their Google account (Google can also obtain this information, which includes a list of Android apps installed on current and past devices along with the firstInstallationTime and lastUpdateTime). This information is also available to users of iOS devices; they can look in the Apple App Store under Account -> "Purchased" to find a list of all iOS apps installed on current and past devices along with the date of installation, associated with a user's Apple ID. *See* for example, Exhibits B.1 and B.2, where I have included the list of apps installed on the two test iPhones.

350. Google likewise has records to determine and/or verify whether a user interacted with an app that uses Google Analytics for Firebase, Ad Manager, and/or AdMob.

351. Google maintains dashboards that show "the number of active projects of Firebase" and "the number of active projects using each of the subproducts within Firebase," including Analytics (Ma Tr. 78:11-25). For example, the Firebase Executive Dashboard "would say the number of monthly active projects given a point in time" (Ma Tr. 142:2-12). Google also keeps records of 28-day active apps using Firebase based on unique app instances (Ma Tr. 142:16-144:23).

352. In its Supplemental Response to Interrogatory No. 2, Google claimed to have "conducted a reasonably diligent search to determine which Android apps of the ones identified in Plaintiffs' First Amended Complaint . . . have had Google Analytics for Firebase enabled." Of the apps identified in the Complaint, Google listed 282 apps that "have had Google Analytics for Firebase enabled" and 80 "apps that have not had Google Analytics For Firebase enabled." Google also clarified that it "can investigate iOS apps as well." This Interrogatory response shows that Google keeps records of the apps that use GA4F, and I am not aware of any reason why Google could not likewise confirm whether or not an app uses AdMob or Ad Manager.

353. Given a list of apps installed on a device and time of installation, Google can look in its records to see whether those apps used Firebase, Ad Manager, or AdMob during the time the user had WAA or sWAA turned off. Steve Ganem likewise explained: "I could look up whether they're using analytics, and what I would probably do is if I had the app ID of that app, I could look up in our internal tools. There's a tool called [redacted] to see whether that app was registered with one of our customers" (Ganem Tr. 133:2-7).

354. To sum it up, Google has records to determine and/or verify (1) which Google account holders turned off WAA or sWAA at any time during the class period, (2) which of those account holders used a mobile device at any time during the class period, and (3) which of those account holders interacted with an app that uses GA4F, Ad Manager, and/or AdMob while either WAA or sWAA was off.

355. In any event, for any user who turned off WAA or sWAA for any portion of the class period, and used Android or iOS devices, the probability of that user being a class member is extremely high. Users typically install a large number of apps on their devices,[173] and users spend a lot of time on apps.[174] Moreover, an extremely large percentage of apps use Firebase, Ad Manager, and/or AdMob. For example, in 2020, Firebase was used [redacted] (GOOG-RDGZ-00060716 at -729).

356. Assuming (very conservatively) that 50% of the top apps use either Firebase, Ad Manager, or AdMob, if a WAA/sWAA-off user uses *n* apps within the class period, the probability of their data being collected and saved by Google is a function *F* of *n*: $F(n) = 1 - (1 - 0.5)^n$. This means

[173] A 2017 document states that [redacted] GOOG-RDGZ-00192217 at -218). [redacted] (GOOG-RDGZ-00064481 at -500).

[174] A 2016 document states, [redacted] (GOOG-RDGZ-00195309 in 2016 at -335) and that "[redacted]. at -336). [redacted] (GOOG-RDGZ-00202401 at -416).

that if a user uses just five non-Google apps during the class period, the probability of their data being collected and saved by Google is at least [redacted] With just ten non-Google apps during the class period, the probability increases to [redacted]. In other words, if a WAA-off or sWAA-off user interacts with just ten non-Google apps during the class period, she has a [redacted] chance of having her data collected and saved by Google.

357. As a further (but unnecessary) check on class membership, Google can use the data stored within its voluminous logs to verify membership in the class. The same records provide information about the volume of WAA/sWAA-off data that Google has collected and saved (to the extent that Google did not destroy or delete such data).

358. As explained above, Google has admitted that "[a]t least one Google log contains one or more bits and/or fields that reliably shows whether specific event-level traffic was generated while WAA was off" (Google's Resp. to RFA No. 25). This means that Google's records can be used to verify whether certain traffic was collected from a WAA-off or sWAA-off user. As discussed in Section VII.B, Google produced information about 16 AdMob-related logs that contain WAA or sWAA bits. Eight of these logs contain non-GAIA data and eight contain GAIA data. Google also produced information about an analytics log [redacted] that contains the sWAA bit, at least in GAIA data. There is also a [redacted] log which contains WAA and [redacted] Google's 2nd Supp. Resp. to Interrog. No. 17).

359. But Google has withheld providing information about the vast majority of logs that contain such a bit. In a court filing, Google represented that "initial searches indicate that, just in the Sawmill repository, one such repository, logs that include the phrases 'waa,' 'swaa,' or 'smh,' contain, in total, over 1 million fields" (Dkt. 250 at 5). But Google has only identified the 18 logs noted above.

360. When a user is not signed into their Google account, Google may also receive the signed-out user's data. Google can readily distinguish signed-out data vs. signed-in data in its non-GAIA logs. As discussed in Section VII.B, Google keeps a record of an account holder's sign-in and sign-out records associated with the user's IP address and user agent, along with time stamp. Thus, Google can determine when a user is signed-in and generated WAA/sWAA-off data from non-Google apps. Furthermore, since Google stores both WAA/sWAA-on and WAA/sWAA-off data from Google O&O apps in GAIA logs, Google can look in its GAIA logs to determine a user's signed-in status. Google also uses a field called [redacted] in its non-GAIA analytics logs, which provides additional verification.

361. I have not yet uncovered any information that there is a WAA/sWAA bit for non-GAIA, GA4F logs; however, a sWAA bit exists in at least one GAIA, GA4F log. WAA/sWAA bits are also stored in ads logs. Since device ID and app instance id are stored in both analytics and ads logs, and since ads logs contain WAA/sWAA bits, one can use the same identifiers stored in analytics and ads logs to determine WAA/sWAA status on an event level. Furthermore, since WAA/sWAA status is determined based on the signed-in Google account, Google's WAA/sWAA status indications inherently indicate that the user is signed in.

362. The upshot is that Google can isolate within its records the traffic generated from WAA-off and sWAA-off users. Google can then use those records to identify and/or verify class members.

363. Another identification method works as follows. For any device that users can still access (i.e., it was not sold, lost, or broken), users can interact with apps that use Google services. Doing so sends identifiers to Google. Google can then use the same identifiers to locate the user's historical data. As I described in Section VII.G of this report, Google can use DSID, ADID, or

IDFA to confirm the associated GAIA ID. The ADID and IDFA can also be used to search for user data within Google's logs and data storage. Alternatively, ADID and IDFA can be used to locate other IDs, such as app instance id, app id, User ID, or PPID. Identifiers such as User ID and PPID can also be located using a user's GAIA IDs, as these 3P sign-in IDs will be present in GAIA logs as well as non-GAIA logs. These IDs can be used to search for user data. As discussed above, Google can take the identifiers in the logs that have been associated with traffic marked as WAA-off or sWAA-off, and then use those identifiers to identify the user.

364. There may also be other encrypted and non-encrypted identifiers common to both GAIA and non-GAIA logs that can be used to locate a user's non-GAIA identifiers and data (*see*, for example, my discussion of encrypted app instance id in GAIA logs in Section VII.G). Though Google's [redacted] graph, even more IDs may be located, possibly from devices that the user no longer has access to. Google can use these IDs to search for user data within Google's logs and data storage (as I have discussed in Section VII.B).

365. The process can also work the other way. Users can provide their identifiers to Google, and Google can use those identifiers to find WAA-off and sWAA-off traffic associated with those identifiers. Broadly, data can be located using the following identifiers or fingerprinting information:

- Non-GAIA identifiers (e.g., app instance id, app id, ADID/IDFA/IDFV/SSAID)
- 3P signed-in identifiers (e.g., User ID, PPID)
- Device information (e.g., IP address, user agent, device model, operating system, screen size, etc.)
- Combination of apps installed on a device

366. Additionally, while sWAA is associated with a user's GAIA account (since sWAA is a Google account setting), Google also associates the sWAA status with Device IDs, which Google

considers non-GAIA.[175] This means that potential class members can present their Device IDs to Google and Google can look up the user's sWAA status using the Device IDs and locate the users' data using the Device IDs.

367. Importantly, Google acknowledges that it identifies users not only by their GAIA IDs, but through their non-GAIA IDs as well. For example, for AdMob Cohort LTV (lifetime value) reporting, Google explains that "To calculate LTV, a basic requirement is to classify events/logs under the same user. It's a prerequisite for data injecting, processing, and aggregating, before conducting an LTV report" (GOOG-RDGZ-00066703 at -712). The same document further explains that "App Instance Id is the primary user identifier used in Analytics" (GOOG-RDGZ-00066703 at -713) and "App instance id is unique in one App. AdMob App id and App instance id are able to identify a user and help us group events by users. For GA integrated traffic, the App instance id is available in Ads logs … Even for privacy users, the app instance id is still available for both Android and iOS Apps. In addition, it's worth mentioning that the [redacted] is also used as the user identifier in GA user baseview" (GOOG-RDGZ-00066703 at -712 (emphasis added)).

368. The methods I have described above for determining and/or verifying class membership can be performed programmatically without any manual work. But to be clear, these methods will only work insofar as Google has preserved the requisite data records. I am informed that Google is preserving the entirety of its records which indicate whether and when a Google account holder turned off WAA or sWAA. But I understand that Google is deleting as a matter of course its

[175] Google's internal documentation explains: "The consent data for [redacted] …users are currently stored in the [redacted] column in [redacted] (GOOG-RDGZ-00207976 at -978), and that: "The following [redacted] have already been propagated to [redacted] (GOOG-RDGZ-00207976 at -980). The ability to check the sWAA status using Device IDs implies that Google located the user's GAIA ID using the user's Device IDs, and populated the sWAA status for subsequent access with the Device IDs.

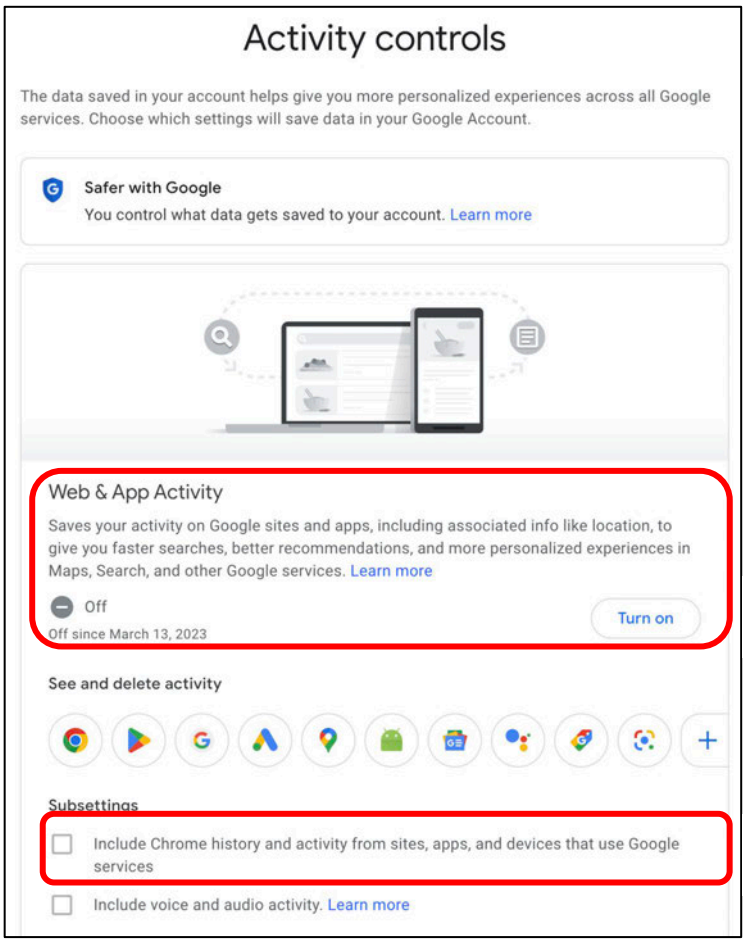
records of event-level app activity data, including data from WAA-off and sWAA-off users. Plaintiffs asked for Google to preserve all records of app activity, but Google refused. Dkt. 185.

J. WAA Functionality: Throughout the Class Period, WAA and sWAA Functioned in Ways that Were Different than Google Represented.

369. Throughout the class period, the WAA and sWAA settings functioned in ways that differed from how Google represented they would function. As discussed in Section VI.B, Google made the WAA and sWAA features available to users in two places: through Google webpages and through the "Settings" menu of a mobile device running the Android operating system (OS).

1. The WAA Switch

370. As discussed in Section VI.B, users can access the WAA and sWAA settings through Google's "Activity controls" webpage.



WAA

sWAA

371. On this page, Google represents that WAA "saves your activity on Google sites and apps," and there is an option for users to "turn off" or "turn on" WAA. In addition, for users who elect to turn WAA "on," there is an option within the Subsettings (sWAA) to "include Chrome history and activity from sites, apps, and devices that use Google services." Users with WAA-on may check or uncheck the sWAA box. But when WAA is turned off, sWAA is automatically turned off and cannot be turned on.

372. The statements Google makes about WAA and sWAA are false as a technical matter. As I have shown, Google does save users' "activity from sites, apps, and devices that use Google services" even when the sWAA box is unchecked or WAA is turned off, including by way of various Google services embedded within non-Google apps (as discussed above in Section VII.B).

373. David Monsees, a 30(b)(6) witness for Google in this case, testified that the reference to "sites, apps, and devices that use Google services" "would include Google Analytics for Firebase" (Monsees Tr. 141:10-13). Similarly, Google's Privacy Policy has throughout the Class Period defined "Google services" to include "Products that are integrated into third-party apps and sites, like ads, analytics, and embedded Google Maps" (Google's 2nd Supp. Resp. to Interrog. Nos. 6-8). Google stores data collected by way of such products, including Firebase, AdMob, and Ad Manager in various logs, as I have described in Sections VII.A and VII.B of this report, and notwithstanding whether WAA and/or sWAA are switched off.

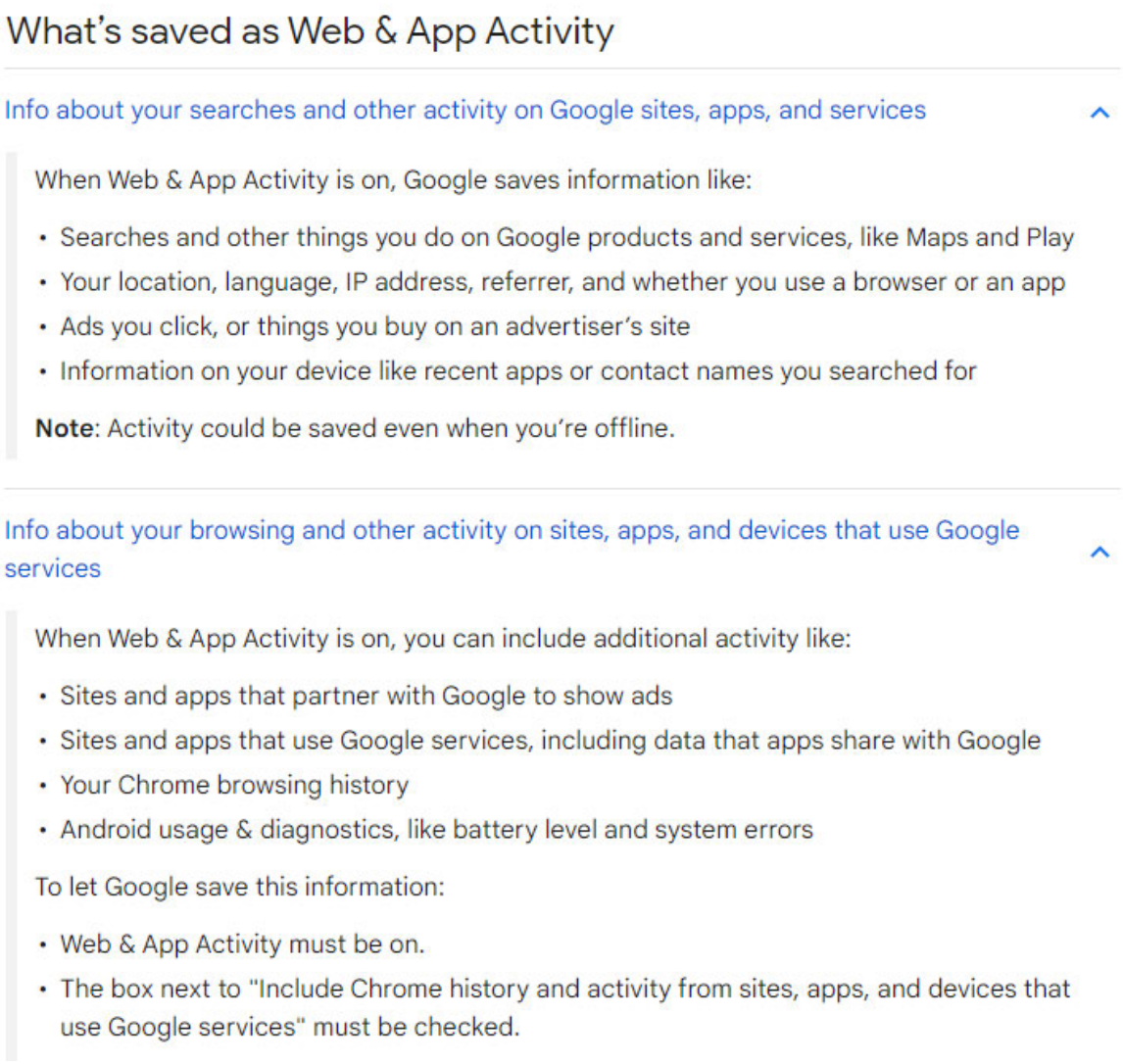
374. I understand that these disclosures within the WAA Activity Controls page have not materially changed throughout the Class Period (Google's 2nd Supp. Resp. to Interrog. Nos. 6-8; GOOG-RDGZ-00208190).

375. Google employees have (correctly in my view) commented on why these disclosures are inaccurate as a technical matter. For example, Google employee [redacted] assessed this

particular "Activity controls" webpage in August 2019 and concluded: "***I don't see how this text can't need modification. An 'on/off' toggle means the off state is the opposite of the on state. If the on state is we log your activity, the off state is we don't log your activity***" (GOOG-RDGZ-00130322 at -322 (emphasis added). Furthermore, other Google documents noted that "choices often presented as binary toggles is ill suited to the nuances and diversity of our services and the people who use them" because "while we know that no two google services require or use data in exactly the same way, the binary toggles that represent our major consent moments belie that nuance" (GOOG-RDGZ-00173600 at -602).

2. The WAA Help Page

376. The "Activity controls" webpage discussed just above in Section VII.J. invites users to click "Learn more," which brings users to the WAA Help page, currently titled "Find & control your Web & App Activity." On this page, Google makes the following representations:



377. On this page, Google represents that, "When Web & App Activity is on, Google saves information like" "[a]ds you click, or things you buy on an advertiser's site." This statement is technically true, but it omits to point out that Google saves this information regardless of whether "Web & App Activity is on."

378. Similarly, to describe sWAA, Google represents that "[i]nfo about your browsing and other activity on sites, apps and devices that use Google services" is "saved as Web & App Activity," which includes activity on apps that use Google services like GA4F, Ad Manager, and AdMob. Google explains that "When Web & App Activity is on, you can include additional activity like:

. . . Sites and apps that use Google services, including data that apps share with Google." These statements are also technically true but incomplete. They omit to point out that Google collects and saves this information regardless of whether WAA or sWAA have been turned off.

379. Finally, Google represents that "To let Google save this information," both WAA and sWAA must be on. That statement is inaccurate as a technical matter. Google is saving this information even if the user has turned off WAA and/or sWAA.

380. I understand that these disclosures within the WAA Help Page have not materially changed throughout the Class Period (Google's 2nd Supp. Resp. to Interrog. Nos. 6-8).

381. Google employees have (correctly in my view) commented on why Google's WAA disclosures are inaccurate. For example, Google employee Chris Ruemmler wrote in a July 2019 email that this WAA Help Page "actually doesn't describe what happens when [WAA] is disabled" (GOOG-RDGZ-00024709 at -710). Mr. Ruemmler pasted into his email portions of the WAA Help Page that I pasted just above, and he explained that "[w]hen Web & App Activity is OFF, I'd expect the opposite to happen." "[G]iven the way on/off works, one has to then assume that ***disabled (off) would be the exact opposite*** of what is described for what happens when the WAA bit is on" (*Id.*) Mr. Ruemmler accordingly recommended that the WAA Help Page be revised because "[t]he WAA and other controls imply we don't log the data, but obviously we do," which gives users "a false sense of security that their data is not being stored at Google, when in fact it is" (*Id.* at -709-710). "We need to change the description to indicate even with the control off, Google retains this data and uses it for X purposes" and to "indicate that WAA-off is identical to being not logged into your account (data logged, but not tied to your account)" (*Id.* at -710-711). This sentiment was echoed by Googler JK Kearns in an email stating that "to me, it feels like a

fairly significant bug that a user can choose to turn off WAA but then we still collect and use the data (even locally)" (GOOG-RDGZ-00044478 at -482).

382. Mr. Ruemmler raised similar complaints over the ensuing months and years. In December 2019, Mr. Ruemmler wrote: "Isn't WAA- off supposed to NOT log at all? At least that is what is implied from the WAA [Help] page . . . So, if WAA is off, how are we [Google] able to log at all?" (GOOG-RDGZ-00130381 at -381). And in July 2020, the same month this lawsuit was filed, Mr. Ruemmler wrote: "Web and App Activity is the worst name ever. This is part of the problem with the WAA bit. What does it ACTUALLY control? It is not obvious at all from our documentation. We need to be very clear about what is controlled by this flag" (GOOG-RDGZ-00089546 at -546). Two years later, Mr. Ruemmler stated that Web & App Activity is "not a great name, but like it could be improved" (Ruemmler Tr. 157:10-11).

383. Mr. Ruemmler explained during his deposition that his questions about WAA and the relevant disclosures arose "back before I had more knowledge about the way WAA works." He believed at the time that "if the opposite of on and off, if it was off, well, we just didn't, you know, send any of this data to Google. But that's not right" (Ruemmler Tr. 72:22-73:1). Mr. Ruemmler likewise testified: "A light is on, a light is off; right? You know, that's the opposite behavior. And so I think I had a misconception that when WAA was off, there was no logging performed" (Ruemmler Tr. 135:20-25); *see also* Ruemmler Tr. 149:3-7 (Mr. Ruemmler testifying that "I believe this is going back to my misconception that WAA off meant no storing of information to Google.").

384. Mr. Ruemmler also conceded that his confusion persisted for over a year. Reviewing multiple emails that he sent over time, Mr. Ruemmler explained that "apparently… didn't know everything it controls because I'm asking the question again" (Ruemmler Tr. 149:22-25; 155:16).

385. I agree with Mr. Ruemmler. To accurately describe the functions of WAA and sWAA, Google must explain that Google collects and saves the same data notwithstanding whether WAA and/or sWAA are off. The only import of switching off these toggles impacts how the data is stored—that is, whether the data is explicitly associated with a user's GAIA ID.

386. Other Google employees have (correctly in my view) expressed similar criticism of Google's WAA disclosures throughout the Class Period. For example, in June 2016, Google employee Jonathan McPhie wrote that "Our definition of 'collect' is more like 'stored' . . . From that perspective, sWAA . . . is more about moving data around and not about 'collecting' more data" (GOOG-RDGZ-00149701 at -701). I agree with Mr. McPhie that sWAA "is more about moving data around and not about 'collecting' more data." Google collects and saves data relating to users' interactions with non-Google apps that use Google services regardless of whether sWAA is on or off. sWAA merely "mov[es] data around"—that is, impacts whether the data is stored in a personal log where it is expressly associated with the user's GAIA ID, as opposed to a non-GAIA log. But in the words of another Google employee, Google is "intentionally vague" about data "collected outside of their Google Account" because "the technical details are complex and it could sound alarming to users" (*Id.* at -702).

387. Relatedly, in November 2018, Google employee JK Kearns wrote "I think teams should not use user data at all if WAA is off" (GOOG-RDGZ-00039094 at -094).

388. In August 2020, weeks after this lawsuit was filed, Google employee Elyse Bellamy asked a colleague whether it was "worth calling out that many people don't feel they have genuine choice? IMO the two problems we face because WAA is so broad are (A) people can't get their heads around what it collects / uses because the scope is - vast and vague" and B) the all-or-nothing nature / lack of a granular controls means people don't feel they have genuine choice if they want

to use Google" (GOOG-RDGZ-00203545 at -546). Another internal Google document related to Google's [redacted] admitted that "much of the [WAA] language intended to be comprehensive feels vague and hard-to-parse for non-engineers / lawyers, and our examples are not universally resonant" (GOOG-RDGZ-00203679 at -680).

389. Internal Google research studies justify these employees' concerns. An April 2017 internal Google study found that the "effect of the activation of the Web & App Activity is not well understood" (GOOG-RDGZ-00020692 at -706). Another seemingly 2017 study (based on the document's metadata) summarized how "8/10 [participants] didn't understand the sWAA text and the effect this could have in their experience" and the presentation described WAA and sWAA as "losers" (GOOG-RDGZ-00144760 at -766). A March 2019 deck titled "Data Retention Usability Study Findings," discussed "persistent points of confusion," including "uncertainty about what type of data is impacted by controls" including WAA (GOOG-RDGZ-00021160 at -182). Similarly, Google user experience research employee Arne de Booij concluded based on yet another study that "WAA settings are hard to understand" (GOOG-RDGZ-00151484 – KeyInsights tab at row 38).

390. The results of an April 2020 study (just months before this lawsuit was filed) are particularly noteworthy. "All participants expected turning WAA toggle off to stop saving their activity" and "All participants expected turning off toggle to stop their activity from being saved" (GOOG-RDGZ-00151992 at -000, -011).

391. That result is not surprising to me because that is exactly how Google described the WAA functionality.

392. Even Google employees with expertise on the Google products at issue in this case have admitted that they do not understand how WAA and sWAA affect Google's collection of the data

at issue. For example, Google employee Francis Ma, who has been involved with Firebase since 2015, including with responsibility for "product management aspects" of Firebase (Ma Tr. 30:13-16, 36:9-37:1) testified that:

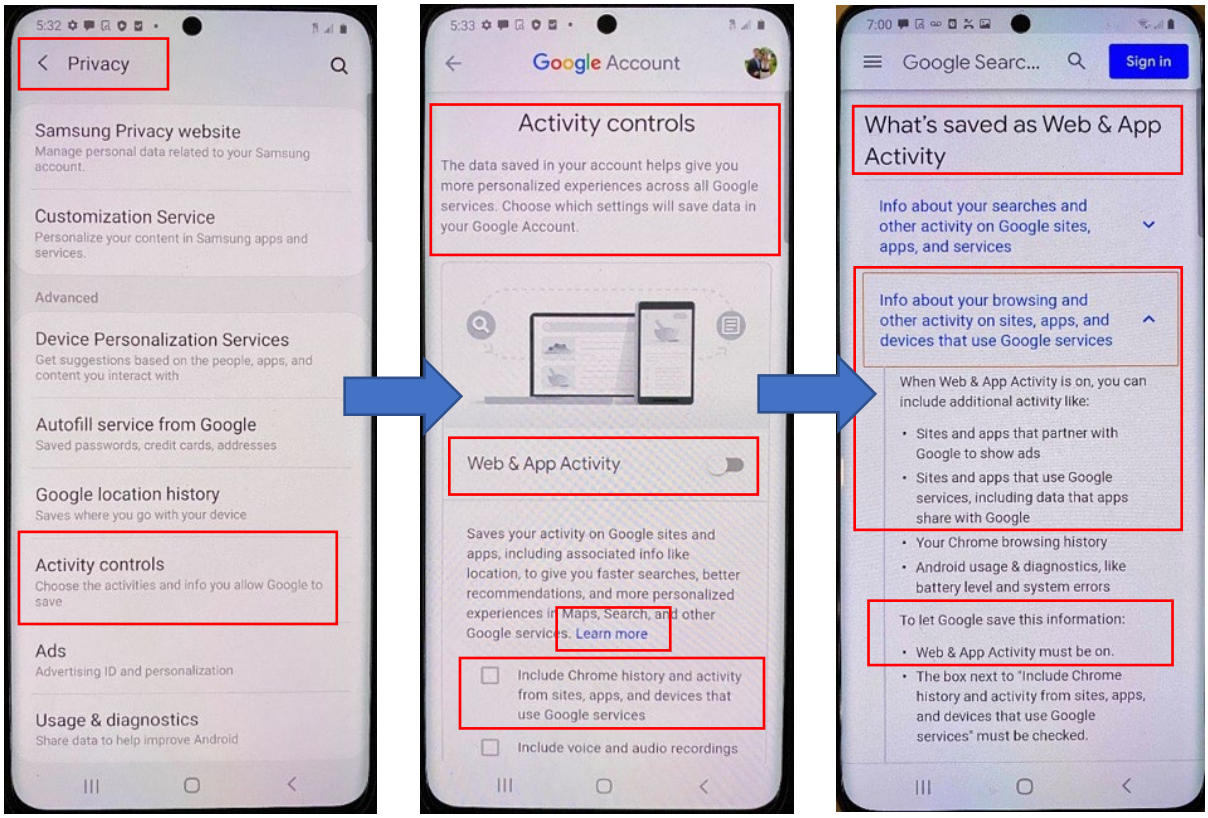
- he does not know if Google saves any data while WAA is turned off (Ma Tr. 62:4-13)
- he has only a "vague understanding" of what WAA is, and is generally not familiar with WAA (Ma Tr. 126:17-19; 127:1-4; 136:16-18)
- he has no idea what SWAA is (Ma Tr. 55:21-56:3; 58:16-24; 119:11-15)

393. Similarly, when asked to describe his understanding of "what the WAA control does," former AdMob product manager Ed Weng testified that "I would have to speculate" and admitted that "I don't know the details behind it" (Weng Tr. 21:17-24). When asked "does AdMob collect data from users who have WAA and sWAA-off," Mr. Weng responded: "That I don't know." (Weng Tr. 143:6-8).

394. Similarly, WAA product manager David Monsees has been an employee at Google for over a decade and has assisted with crafting the WAA disclosures but could not provide a yes or no answer when asked if sWAA-off data is stored by Google (Monsees Tr. 287:19-290:11).

3. Android Screens

395. The same WAA disclosures I discuss in the immediately preceding subsections (within the "Activity controls" webpage and the WAA Help Page, are made available to users through the "Settings" menu of a mobile device running Android OS. Users can navigate here to switch off WAA and/or sWAA, where they are informed by Google:



SCREEN 1 SCREEN 2 SCREEN 3

396. Screen 1 of the settings menu represents that users are able to "choose the activities and info you allow Google to save," and clicking this option brings users to the "Activity controls" screen where the WAA and sWAA features are located. That statement is inaccurate because switching off WAA and/or sWAA does not prevent Google from "sav[ing]" users' activity data. Google saves that data regardless of whether WAA and/or sWAA are switched off.

397. And the disclosures on Screen 2 and Screen 3 are inaccurate for the same reasons discussed above. The language on Screen 2 matches the language on the Google "Activity controls" webpage (*see supra* Section VII.J.1). And the language on Screen 3 matches the language on Google's WAA Help page (*see supra* Section VII.J.2).

398. I understand that these disclosures within Screens 1-3 have not materially changed throughout the Class Period (Google's 2nd Supp. Resp. to Interrog. Nos. 6-8; GOOG-RDGZ-00208190).

399. I also understand that the language on these screens was controlled by Google throughout the Class Period. Mr. Monsees (Google's 30(b)(6) designee) testified that Screen 2 "is a Google screen regardless of the OEM device that the user is using" (Monsees Tr. 239:24-240:1). And Screen 3 "is also a Google-owned help center page not controlled by the OEM" (*id.* 240:6-8). And counsel for Google has admitted that Google likewise controlled the language on Screen 1 throughout the class period.

400. Despite all of the employee complaints recounted in the prior subsections, Google has not revised its WAA disclosures to explain to users its true functionality—namely, that Google will save users' activity data regardless of whether they turn off WAA and/or sWAA, and that switching off those toggles merely affects how Google stores the data—not whether it's stored in the first place.

4. "My Activity"

401. For most of the Class Period, Google within its Privacy Policy represented to users that they could visit "My Activity" to "to review and control data that's created when you use Google services" (Google's 2nd Supp. Resp. to Interrog. Nos. 6-8). This provision also provides a hyperlink to a Google webpage where the WAA toggle is located, in addition to two other Google toggles: Location History and YouTube History.[176] That representation is false as a technical matter because Google does not provide any control which allows users to prevent Google from collecting and saving data generated from their use of non-Google apps.

[176] *Welcome to My Activity,* Google My Activity, https://myactivity.google.com/myactivity?utm_source=pp (Last accessed February 15, 2023).

402. Google as of February 2022 updated its explanation of My Activity in the Privacy Policy: "My Activity allows you to review and control data that's saved to your Google Account." This updated description is incomplete because Google does not explain that it will collect and save data tied to Google identifiers regardless of whether users turn off WAA.

403. Moreover, the Privacy Policy incorrectly states that "across our services, you can adjust your privacy settings to control what we collect and how your information is used," and that such "[p]rivacy controls" include the "Activity Controls" (e.g., WAA). That statement is false as a technical matter because WAA does not allow users to prevent Google from collecting and saving the data they generate from their activity on apps that use Firebase, AdMob, and Ad Manager.

404. Google CEO Sundar Pichai has misrepresented Activity Controls, including to Congress. For example, Mr. Pichai testified to Congress on December 11, 2018 that within "My Account," users can "clearly see what information we have" and "we give clear toggles by category where they can decide whether that information is collected, stored."[177] Mr. Pichai also testified that "we give you the choice of whether you want to store the data or not" and that "We are pretty explicit about data which we collect and give you protections for you to turn them on or off."[178]

405. These statements from Mr. Pichai, as well as the Privacy Policy's statement about "My Activity," are inaccurate as a technical matter. None of the toggles that Google offers (including WAA) "give you the choice of whether you want to store the data or not" and no toggle allows users to "decide whether the information is collected [and] stored." By way of code embedded within non-Google apps for at least Firebase, Ad Manager, and AdMob, Google collects and saves

[177] *Live: Google CEO Sundar Pichai Testifies on Data Collection (C-Span)* at 45:40, YouTube, www.youtube.com/watch?v=WfbTbPEEJxI (Last accessed February 15, 2023).
[178] *Id.* 2:11:05, 3:33:31.

information about users' app activity regardless of what they do with their My Account toggles.[179] Indeed, the founder of Google's Privacy and Data Protection Office, Eric Miraglia, testified in this case that he is "not aware of any setting" that users can employ to prevent Google from collecting data relating to their app activity. Miraglia Tr. 97:4-6.

406. Relatedly, there is no way for users to review and delete the WAA-off and sWAA-off data that Google is storing. Greg Fair, a former Google employee, explained during his deposition that "I'm not aware of a specific control that the user can delete something from Google. The controls that we have in in the My Activity space talk about deleting a piece of data from your account" (i.e., only data explicitly tied GAIA (Fair Tr. 79:6-10)).

* * *

407. As explained in this section, Google employees share my view that Google's WAA disclosures are inaccurate as a technical matter.

408. Below, I provide additional examples of Google employees expressing concerns about WAA and sWAA and other Google privacy settings, focusing on whether Google has accurately described what they do and do not do.

- "Google's own systems have become more complex over time, making it much harder for people to make decisions related to privacy." GOOG-RDGZ-00025811 at -812).
- "WAA just isn't clear to users" (GOOG-RDGZ-00090236 at -239).
- Google's promise of "control" is "just not true" (GOOG-RDGZ-00020680 at -680).
- "[W]e're stretching ourselves thin, especially given…a system that is just fundamentally difficult to get (WAA)" (GOOG-RDGZ-00129096 at -097).
- "It is not only our consent that is too convoluted, the underlying approach and systems to capturing and using data is as well" (GOOG-RDGZ00129042 at -043).

[179] In its Response to Interrogatory No. 1, Google stated that "a user turning off Web & App Activity does not prevent apps from collecting data via Google Analytics for Firebase . . ."

K. WAA Changes: Google Could Change WAA and sWAA to Ensure They Function as Described. Google Could Also Purge its Systems of WAA-off and sWAA-off Data.

409. It is my opinion that Google could change WAA and sWAA so they match their function as described in Google's disclosures. Put differently, Google could change WAA and sWAA so that WAA and sWAA actually do the work that Google says they do. Google could also change its processes going forward to (1) stop collecting and saving WAA/sWAA-off data, (2) purge its systems of WAA/sWAA-off data already collected, and (3) delete any products, services, or algorithms built in whole or in part with WAA/sWAA-off data.

410. Google has the logging infrastructure in place to honor the WAA and sWAA controls (i.e., to not collect and save WAA-off and sWAA-off data).[180] As discussed above in Section VII.B, as part of its process for collecting and saving each analytics and ads event, Google relies on a consent checking infrastructure to determine WAA/sWAA status. A change in Google's logging infrastructure would be to not save the data where this consent check determines that WAA or sWAA is set to off.

411. [redacted] GOOG-RDGZ-00043133 at -133). Put differently, Google has in some cases decided that sWAA should function as advertised—that is, for some Google products and services, the act of switching off sWAA does in fact stop Google from collecting and saving the data. But for other products, including the analytics and ads products at issue in this case, sWAA merely affects how the data is logged (contrary to Google's representations). That sWAA in some

[180] GOOG-RDGZ-00046271 at -278. [redacted] Monsees Tr. 261:23-262:10.